Research Report 6: Audit Report

What did you do?

An audit plan template was provided for this assignment. Here I filled out the blank information and the blanks in the audit plan that referred to what we will need to be checking when completing the audit. I was able to complete the audit on a small medical business.

I did use most of the descriptions from the audit plan example provided in the attached documents and what was discussed in the assignment video. I added a few more points to check that I could see might not pass and needed to be made aware to the business.

What were the results?

Out of the eighteen points that were checked on the audit plan, three of them did not pass. The first being password strength. Due to the password being weak and the passwords being written down in their notes, I did mark this one as failed. Since I could see that computers were being unattended in the facility, I added a point in the audit that asked if computers were being locked with a password when unattended. The designated employee did state that they personally do lock their computer, but that other employees do not. I would not consider these first two points that failed 'severe' due to the point of access being controlled on all business systems passing. There is no customer access to be able to access these unattended computers or expose passwords, but there is always the chance of another employee accessing files/computers they do not normally have access to.

A point I added as well in the audit plan was checking whether employees are aware of phishing emails and how to recognize them. Personally, when email is being used often in a business, it's important for employees to know when emails are suspicious and could be trying to gain vital information. The designated employee that I spoke with stated that not all employees are knowledgeable when it comes to phishing emails. I did mark this one as failed due to employees continuously clicking on phishing emails. The designated employee did state that there are modules provided to other employees on the risks of phishing emails and how to recognize them.

Other important points that passed that I found important was making sure there was an inventory for the devices of the organization, and I was surprised to find out there was one that existed. Because of this, there were no other digital devices found or needed to be discovered. One part of the router location that was not 100% okay was that the temperature varies where the router is located. For the most part, the temperature is good for the router, but occasionally it can get humid. Another good point that passed was that auto updates are on ensuring that devices stay up to date.

What are the recommendations?

My recommendations include talking points for password strength, procedures for leaving computers unlocked when unattended, and being aware of phishing emails. These were the three points that failed. Regarding the password strength, I did recommend making the password stronger by adding numbers and special characters. I also stated that it is best practice to

regularly update these passwords and to set a reminder, however often preferred, but no longer than six months. I also pointed out that it is best not to have these passwords written down, to lower the risk of someone unauthorized gaining access.

When it comes to computers being left unattended with no lock, I did recommend notifying all employees of the risks that may come with that. I stated to the designated employee that it is best practice to keep the computers locked when unattended, with them being password protected. Yes, if employees are not used to this, it may take time, but it is of vital importance to prevent important information from being exposed.

It is good that the employer has modules in place to keep employees informed of phishing attacks, but I also recommended quizzes that were provided to me in a previous class. These quizzes will give real life examples of phishing emails that I feel match closely with the ones employers have been getting to their email. The designated employee was able to show me a screenshot of one of the phishing emails. These quizzes will test how well a person is able to recognize these attacks.

What is their risk posture?

Looking at the bigger picture, the most important points of the audit plan did pass. For example, it is good that the business had security plans and backups in place as these are some of the prioritized components when it comes to a recovery plan. There was an outage plan that the designated employee stated was out of date and needed to be updated, this could lead to a vulnerability in the business' attack surface. Another important access that lessens the business' risk of a breach, is that access is controlled on all business systems and files. Overall, the business' risk posture is not severe, but can use some help when it comes to minor vulnerabilities. The greatest risk for the business is their employees not being knowledgeable of the vulnerabilities that are created by them. The greatest vulnerability of the business is leaving computers unattended and weak passwords.