CYB 201 FINAL PROJECT & ESSAY

**Result Summary**

First off, my overall score was 770 which is on the high end of what is considered "good" or acceptable. This score is also above the average for the United States which is at the low end of good which I find hard to believe. Most likely the results are biased since the majority of people taking a cybersecurity exam have better than average security habits.

Topic 1: Household Computer Safety - I was at a "fair" score which is most likely the result of my answering no to the question of "do you have virus scan software on all computers". This could be an area of improvement but since none of the devices that contain sensitive information are on the same network as most of the home computers, I find it okay. Both mine and my father’s work computers have their own VPN and virus protection so they are good.

Topic 2: Using the internet Safely - I was between "fair" and good for this one. One of the problem areas was that I don’t "logout" of my accounts after using them. Since I use a password manager anyways, I don’t consider this to be an added layer of protection since anyone with my browser login, which is 2 factored, could get into any non-sensitive account I have.

Topic 3: Choosing and Protecting your Account login - For this one as was almost at the halfway point between good and excellent. The main negative was that I let my password manager and google remember passwords. This is definitely an obvious negative but is not avoidable with how many different accounts I have and then having different good passwords for each.

Topic 4: Securing Mobile Devices - My security here was great at the top rating so no problems there.

Topic 5: Securing Wi-Fi - I was given a "good" rating for this, the one negative is that the Wi-Fi passwords don’t change frequently enough. Could easily be improved if I lived by myself but since I don’t I have to consider other people and the fact that over 50% of our devices are smart and need Wi-Fi connection. So, if I changed the password, I would have to reconnect all of those which is over 10 at this point. Not going to happen.

Topic 6: Securing the Wi-Fi/Network Router - My security here was great at the top rating so no problems there.

Topic 7: Backing Up Data - My security here was great at the top rating so no problems there.

Topic 8: Smart Devices and the IOT - My security here was great at the top rating so no problems there.

Topic 9: Physical Security - My security here was great at the top rating so no problems there.

Topic 10: Breach and Incident Response - This was actually one of my lowest scores with another "fair" rating. The recommendations were to keep a maintained list of technology I own to keep better track of the security on them. Technically I do it’s in my head. Next was my level of understanding of cybersecurity issues. I could go either way on this advice since it is kind of relevant since I don't have any alerts, but I trust my work IT team to alert us when something is worth noting. Then that notice would transfer over to my personal devices as well. The last suggestion that was made was to put a freeze on my credit which I will take into consideration but is not likely since I’m at a key point in my life where my credit will be accessed a lot. Something to look into further.

**Data Security Challenges**

Challenge 1:

Problem definition: The increased needs to have higher security whenever a new risk is established. By this I mean whenever a new threat or standard is put into place for security all of my security has to change with that. The ever-changing landscape of technology causes your security protocols to be constantly updating.

Example: Basic password cracking has improved tremendously the last 10 years due to computer power which has increased the need for better passwords but soon it will change again.

Solutions: The only possible solution to avoid this challenge is to have security measures that are constantly updated by themselves. So having security services that are implemented by professional organizations etc.

Challenge 2

Problem definition: Since my job is remote and involved in many outside sources my access to outside systems for work devices is higher than normal.

Example: This can be anywhere from internal servers with data sharing to as far as external systems that I need access to. I can’t be specific on some of them, but simple instances would be for external data exchange services where multiple users are hitting a single source and constantly downloading and uploading data/files.

Solutions: There is really a solution to this since it is required for my jobs functionality but in order to maintain this use case while staying secure all required systems that I need to access should be secured and constantly check by our IT department.

Challenge 3

Problem definition: Not having an option but to enter my data into a system.

Example: This is most common on online stores, etc. but also for my work accounts and social accounts. Although I do restrict information that I would view as personal there is a certain level of personal information that is almost required now days to be efficient on the internet.

Solutions: One possible solution is that I construct multiple identities, being careful to never reveal real information about my true self unless absolutely required. Solution two is to just be mindful of what information you have out there in its entirety. I know for lots of people you can easily forget that you have some information here and other information there and if someone where to put it together its actually quite private.

**How could this assessment effect a large organization?**

This depends on the implementation that they are taking the assessment. This assessment could be taken by the entire company, or it could just be taken by a head of IT to evaluate their system. Either way there would be some overlap with the questions that were ask in this assessment, mostly about internet and email safety. The more in-depth device, incident response and networking devices would be more fit for the IT departments assessment.

Personally, I would recommend that the entire company takes an assessment because then you will get an entire picture of what everyone is doing. And as we know the biggest failing point of a large company for its security is its employees. The assessment results could then be reviewed and used in a new plan that IT can construct and implement to better the company security.

Most likely if the questions were created correctly for the company’s scenario you might be able to find major security flaws, most likely in access levels.