**Name:** Coral S. Schmidt Montilla **ID:** 148830

**Objective:**

Upon completion of this activity, you will be able to analyze data about cybersecurity for a given context-setting and create a cybersecurity assessment for a small network.

**Student Instructions:**

Create an audit of your home personal area network. Identify assets. Evaluate them using the model provided in this module to establish priorities. Make at least three recommendations based on your findings. This activity is an assignment. This activity is worth 20 points. You will have 1 opportunity to complete the activity.

My home network supports a mix of school, work, and entertainment activities, and it includes both wired and wireless connections. It’s used daily by multiple people in the house, including my 1 roommate and almost daily by other guests, which increases exposure. To reduce that risk, we have three Wi-Fi networks in place, RSK, RSK VoIP, and RSK Guest, as well as wired Ethernet connections for high-priority devices like our Smart TV, all gaming consoles, my dad’s company computer, and my brother’s laptop. For this assignment, I evaluated all devices using the ALE (Annual Loss Expectancy) model from Module 11 to identify the highest-risk assets and recommend ways to protect them.

The network includes two college laptops, one desktop computer for my dad’s company work, two smartphones, two tablets, a printer, smart appliances (vacuum and washing machine), a Smart TV, two Xbox consoles, a Nintendo Switch, one Google Home, and three Google Casts. We also regularly use OneDrive and Google Drive for cloud storage, and all devices are kept up to date.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Value ($) | Exposure Factor | SLE (Value × EF) | ARO | ALE (SLE × ARO) |
| Computer | 1,200 | 0.9 | 1,080 | 0.9 | 972 |
| Smartphones (x2) | 1,600 | 0.7 | 1,120 | 0.6 | 672 |
| Laptops (x2) | 1,800 | 0.75 | 1,350 | 0.5 | 675 |
| Wi-Fi Router | 300 | 1.0 | 300 | 0.8 | 240 |
| Xbox Consoles (x2) | 900 | 0.5 | 450 | 0.4 | 180 |
| Nintendo Switch | 300 | 0.5 | 150 | 0.3 | 45 |
| Smart TV | 600 | 0.6 | 360 | 0.4 | 144 |
| Tablets (x2) | 700 | 0.6 | 420 | 0.5 | 210 |
| Smart Devices (IoT) | 1,100 | 0.4 | 440 | 0.3 | 132 |
| Printer | 250 | 0.4 | 100 | 0.5 | 50 |

The assets with the highest risk are my work computer, smartphones, and the college laptops. These devices contain sensitive data or are used for work and school, making them targets for unauthorized access or malware. While devices like the consoles and smart appliances are lower on the list, they still connect to the internet and can serve as potential entry points if not secured properly.

**Recommendations:**

1. **Continue Network Segmentation and Wired Prioritization:** Keep using the separate networks (RSK, RSK VoIP, RSK Guest) and wired connections for high-priority devices. This helps limit exposure and control traffic flow.
2. **Apply Multi-Factor Authentication (MFA):** Make sure all cloud accounts used for school, work, or storage are secured with MFA in case login credentials are ever compromised.
3. **Regularly Monitor Router and Device Logs:** Since multiple people use the network, keep an eye on router logs and connected device lists to detect unfamiliar access.

This assessment helped identify which devices carry the most risk and showed how important it is to use structured security methods like network segmentation and MFA. The combination of wired and wireless access, along with a mix of user types, makes it even more important to review exposure regularly. Keeping things updated, controlled, and logged goes a long way in protecting the home network from everyday threats.