Week assignment

Kenneth Anderson IS 4670 Week 1 Assignment 2 After reviewing the new network design, we have seen several threats and came up with countermeasures to prevent these attacks. The first threat is the connection between the internet and the company's router and connection between the wireless router and switch. Hackers, viruses, and mallard can easily get in through this connection and infect the network. The countermeasure for this is a firewall or intrusion detection system. This equipment will help detect any unwanted guests the get onto the network.

You can control what traffic moms in and out of your network. Next would be the wireless router being unsecured. If this router is left open and SAID board casting, any within its range can access the company's network. A countermeasure for this is password encryption and stealth id. Hiding the id of the router will allow it to be hidden from anyone scanning for wireless routers to use. Encryption password puts a lock on the router to where only people with the key can access the router. The last threat would be the workstations and laptops. Users make the most mistakes on these machines.

They download and go to places they shouldn't which causes the risk of viruses and hackers. Countermeasures are Anti Viruses, patches, and teaching. Anti-viruses will help protect against viruses and mallard that can allow hackers to enter the system and still information. It's important to keep the definitions up to date so the VA can protect against the latest viruses. Updating SO with patches can also prevent security threats. Teaching users the dos and don't of security issues can help them be aware of the threats and what they should do to help prevent risks from occurring.