CYS 310 Writing Assignment 1: Application of Risk Management Techniques

Kaleb Alstott

To start off one of the first threat/vulnerability pairs I see is all three sites using Ethernet-cabled local area networks (LANs) to connect the users to the industry-standard managed switches. I love the idea of using LANs to connect people to the work area but there is a possible threat here in which is making sure people are signed in as who they are and have the correct protocol and hierarchy to the files that they are intended to have. The vulnerability or weakness in this case is having all the LANs connected to the three main sites. This is the weakest threat/vulnerability we have and would list this as a minimal threat as of right now.

I feel as if the best way to approach this risk is to handle it is with the least mitigation approach. This is a very simple vulnerability that takes no time to fix. All we must do is create the correct active directory functions such as having the correct users/groups protocol assigned correct to what files they will be needing for their work. I’d also make sure all employees have a password to sign into their ID with so, we can double check and make sure you are who you say you are. I’d make sure there was no repeat passwords or passwords with little to no strength for increased security. I still agree with using the ethernet cables to connect all our employees as opposed to wireless, but we need to make sure that our people are signed into as who they are supposed to be.

The second threat/vulnerability I see next is that “the remote production facilities connect to headquarters provided by an external Internet service provider (ISP) and share an Internet connection through a firewall at headquarters.” The vulnerability in this situation is that we are currently assigned to an ISP that we as a company could be sharing with other people. This is not a private network that just the company is using and even with the firewall in place to protect us from other users on the ISP I think we should be on a private internet service provider. The threat here can occur if the wrong person is on the ISP and just so happens to break through our firewall. As slim as this is I’d rather be safe than sorry and have our own private ISP, so we know who is on our internet and what is going on with our company and employees not just the random people assigned our public ISP. I would rank this risk at a medium level risk. Something we need to keep an eye out for and maybe change soon but nothing we can’t bounce back from if worse comes to worse.

After looking over the risk vulnerability here I would say the best risk handling strategy I’d use here would be the transfer/sharing technique. I feel as if our company passing over our ISP to their company and asking for a private safer network would be an acceptable use of a third party. Having a third party take care of our internet troubles and having all our employees on a private internet source rather than a public one will limit the access people have to our network. All in hopes of keeping our employees all on the same internet service that we can monitor and track if need be.

The last and final threat/vulnerability I see that is the most important and is ranked as a high-extremely high risk is that we have salespeople all around the country connecting to our VPN through their own personal internet connection in their home offices. The vulnerability that is at hand here is a lot of these at home offices have little to no security. We have no protection for all these workers across the U.S. besides there VPN. This can be a huge threat to us due to the impact of how much data we would lose about our customers and about ourselves.

For our last vulnerability and our biggest one we would use the mitigation technique to handle this situation. There is multiple of different ways we can approach this and fix it but we can handle most of our issues here with group policy objects in active directories. One would be to train our employees to be up to date with how to spot phishing emails, malware, stronger passwords, etc. If we transfer over to the private ISP this will help us our tremendously knowing we only have people for our company on our internet service provider, making other users stick out like a sore thumb. Finally, I think we should talk about how to increase our technical environment from the home office. We can start off by restricting work hours in which our data can be accessed. Moving on I think the company keeping antivirus software up to date and mandatory, separate work and house technologies, encrypting devices or files transferred, and lastly having a strong secure WIFI. We can also secure WFI in home workspaces by enforcing bit/applockers to prevent many from clicking and going to websites that can leave an open access for hacking into our network. We would also have to make sure these employees working from home have strengthen passwords, expiration passwords, no reusable passwords, and on top of that maybe even a two level authentication factor such as a fingerprint that way we know who the user is logging in is actually the employee. With such a big vulnerability and such a high risk of this scenario happening I feel as if we should hope on this security improvement immediately so we can protect our at home workers asap.

Resources

Managing risk in information systems book pages 20-25

<https://www.businessnewsdaily.com/9372-secure-home-office.html>

(talks about increasing security at home)