Data Center Security Controls Plan

Emily Kellogg

University of Advancing Technology

Data Center Security Controls Plan

Each and every company implements a security controls plan. Security controls are put in place to mitigate and protect an organization’s data and physical property from security risks. Although there are several to choose from, only three controls will be chosen for my organization’s plan. Those controls include internet safety, antivirus software, and password management.

# My Plan in Detail

### **Internet Safety.**

Internet safety is defined as “the practice of following actionable guidelines, understanding modern technology, and protecting your digital devices so you can defend against the malicious parts of the online world” (Applied Educational Systems, n.d.). One way to implement this control is with user training. By training everyone on internet safety procedures, they become aware of acceptable and unacceptable internet use at work. Training could include acceptable use of company property like computers and issued devices, acceptable use of personal devices like smartphones (while working), and acceptable use of remote devices when working from home. It could even require attendees to sign an acceptable use contract once they finish training, so they become legally liable for their actions on the internet.

Tulsa World has an article on internet safety rules for the workplace. They provided several important rules for employees to follow when working. These include making sure phones are password-protected and passwords are stored away securely, never leaving a smartphone unattended and unlocked, only visiting secure sites, using firewalls, reporting suspicious activity to IT, keeping information secure, and protecting oneself from email scams (Carroll, 2019) . As simple as these rules are, they are vital to the protection of company data. If even one computer becomes unsecure in a network, the entire network becomes vulnerable.

#### Antivirus Software***.***

Antivirus software is an important tool that should be downloaded on every device necessary within a company. Norton (2019) explains the importance of antivirus software:

“Antivirus software helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware as quickly as possible.”

Some AV software’s come with the purchase of an OS, like Windows 10’s Microsoft Defender. Others can be bought for corporate use, like BitDefender GravityZone (Turner, 2021). Implementation could include choosing and downloading the appropriate AV software to each device within the network and customizing it based on the company’s needs. That way, the entire network would be monitored and protected from viruses, malware, and other vulnerabilities.

##### **Password Management***.*

This final methodology may seem self-explanatory, but it goes further than making strong passwords (see Figure 1). Password management is all about securing passwords from unauthorized access and use. Not only should employees have strong passwords, but they should also protect those passwords from others. Examples of protecting passwords include never sharing passwords with anyone, especially through text or email, and using a password manager. It does not matter if the person asking for the password claims to be IT or a manager, passwords should never be shared.

Two methods of implementing password management include adding password management to the user training course mentioned above and conducting password audits. The password management section of the course would cover the danger of phishing emails, malicious emails that are used to steal personal information like passwords. It would also include basic password safety like the creation of strong passwords, not reusing passwords, using password managers, and not sharing passwords with anyone. The password audits would be used to track employee passwords to see if they are complying with company policy regarding passwords (Data Privacy Manager, 2021). Both user training and password audits are necessary for the protection of company data because passwords are used to secure almost everything.

Diagram

Description automatically generated

Figure 1: 5 Tips to Improve Password Security in the Workplace (Data Privacy Manager, 2021)

All companies have their own unique security controls in place to ensure that their data and network are constantly protected. They can be as simple as internet safety courses, or as intricate as antivirus software. Upon researching 3 security controls of my choosing, I found password management to be the most interesting because there are so many factors that go into it. Audits, training, protection, etc. It was very interesting to learn about. On the other hand, though, every methodology I researched was interesting because the guidelines to follow for each change between personal use and company use. For example, antivirus software. I can get away with using the default antivirus on my home system, but as an IS professional in an organization, I need more customization and control to protect the network. Overall, I chose and researched three (of the many) security controls and created a plan for my organization based off them. If I had to do it in real life, I most likely would have chosen more than three controls because networks are needy.

# Bibliography

Applied Educational Systems. (n.d.). *What Is Internet Safety and Why Is It Important to Teach?* Retrieved from Applied Educational Systems: https://www.aeseducation.com/computer-applications/what-is-internet-safety

Carroll, K. (2019, July 7). *Business Viewpoint: Internet Safety in the Workplace*. Retrieved from Tusla World: https://tulsaworld.com/business/business-viewpoint-internet-safety-in-the-workplace/article\_1f92d2ee-a1a4-525f-92da-a3be00563418.html

Data Privacy Manager. (2021, August 24). *How to Improve Password Security in the Workplace*. Retrieved from Data Privacy Manager: https://dataprivacymanager.net/how-to-improve-password-security-in-the-workplace/

Data Privacy Manager. (2021b, August 24). [5 Tips to Improve Password Security in The Workplace, Image]. Retrieved from https://dataprivacymanager.net/how-to-improve-password-security-in-the-workplace/

Reason. (2020, January 12). *Why Is Antivirus Software Important?* Retrieved from Reason Blog: https://blog.reasonsecurity.com/2020/01/12/why-is-antivirus-software-important/

Turner, J. (2021, May 16). *The Best Antivirus Software for Business*. Retrieved from Tech.co: https://tech.co/antivirus-software/best-business-antivirus#bit