Cyber Security Policy

Larry Le

Department of Cybersecurity, Old Dominion University

CYSE 300

Joe Kovacic

January 24, 2024

Cyber Security Policies

In this paper I will discuss what security policies are and why they are important. Then I will discuss five of my most important issues that should be addressed in the security policy.

Defining Security Policy

In almost every business in today's society they use some form of technology. Whether it is desktops to do work, point of sale machines to process payments, or even mobile apps to execute a service. All of these examples are vital to continue the business but without a security policy we are at risk to attacks from hackers. According to Garth, "A company cyber security policy helps clearly outline the guidelines for transferring company data, accessing private systems, and using company-issued devices" (2023). This just means that they provide a framework for consistent decision making and behavior. After careful consideration my five most important security policies are; password requirements, acceptable use policies, disaster recovery, incident response and security awareness training.

Password Requirements

I think the one of the easiest ways we can deter password attacks from happening is just to implement a good password policy. According to Paul and Aithal, " From the top 10 most common database security issues, weak and blank passwords make up about thirty five percent of the issues" (2019). The least that we can do is implement some basic password procedures. Some characteristics that I would include are password length, complexity, reuse, expiration and age. Length I would recommend more than 12 characters. Complexity would be a mixture of lower and uppercase letters with special characters. Password reuse is making sure that the same password can't be used for multiple accounts. Password expiration is changing the password after a specific period and password age refers to the time a password has been in use.

Acceptable Use Policy

According to Kirvan, “An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network, the internet or other resources. Many businesses and educational institutions require employees or students to sign an AUP before being granted a network ID” (2022). This is important because the AUP outlines the do’s and don’ts for users when interacting with an organization’s IT system. It also protects an organization from legal issues and security threats.

Disaster Recovery

In a perfect world we wouldn't have to worry about this but some days aren’t our days. A good security policy will have to plan for the worst and when that does happen they need to outline how to recover from these events or disasters. Disaster recovery policies focus on data recovery after a disaster. For example, say the company is located in Florida. Florida is susceptible to hurricanes. Some hurricanes are mild but what happens if one just levels the area. We need a plan to outline what to do in this scenario and how to get our services back online.

Incident Response

According to Business.gov, “ If a cyber security incident occurs, you should minimize the impact and get back to business as soon as possible. You’ll need to consider: how to respond to a cyber incident, what actions to take, staff roles and responsibilities for dealing with a cyber attack” (2024). What that means is that the incident response outlines the approach on how to manage and mitigate security incidents effectively. Knowing what exactly to do in these instances will ultimately speed up our response time and save money.

Security Training

Lastly but most important would be security training. According to Terra, “ The cost of cyber-crime averaged $11.7 million in 2017 and $13 million in 2018, a rise of 12-percent, and an increase of 72-percent over the past five years” (2023). Employees are still one of the biggest vulnerabilities in any organization. Keeping people properly trained on common social engineering tactics or common forms of cyber attacks can save the business millions. Imagine you buy a Lamborghini. It can go zero to sixty in 3 seconds, it looks immaculate but you can’t get it out of first gear. No matter what the car can do, not being properly educated on how to use it will waste all the perks of having it. The same can be said about our cyber security. No matter what kind of firewall or encryption you use, if an employee opens the wrong email then the hacker will get in with ease.

References

Coulson, G. (2023, November 29). *Cyber security policy*. Betterteam. https://www.betterteam.com/cyber-security-policy

Create a cyber security policy. Support for businesses in Australia. (2024, January 18). https://business.gov.au/online/cyber-security/create-a-cyber-security-policy#:~:text=A%20cyber%20security%20policy%20outlines,protecting%20them%20and%20your%20business.

Kirvan, P. (2022, June 13). *What is acceptable use policy (AUP)? - definition from whatis.com*. WhatIs. https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP

Paul, P., & Aithal, P. S. (2019). Database security: An overview and analysis of current trend. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3497728

Terra, J. (2023, August 7). *Why is security awareness training important?*. Simplilearn.com. https://www.simplilearn.com/importance-of-security-awareness-training-article