Corporate Information Security Policies

Dennis Hargro Jr

Old Dominion University

202220_CYSE300_34271 INTRODUCTION TO CYBERSECURITY

Professor Malik A. Gladden

January 29,2023

In a world revolutionized by internet technologies, there are bound to be those who wish to make gain by exploiting the less aware users and the vulnerable systems and applications that have become a fundamental part of the engine that keeps the working world moving. In the business world, where sensitive information is abundant, we must apply the most up-to-date defenses and policies to deter attackers from accessing such information.

If I were to create a security policy plan for a corporate system, I would look towards such issues as: employee access and password management, limiting unnecessary activities on work systems, limiting the use of outside devices with the work systems, devising how long sensitive information is held within the system, and keeping a post incident report.

Learning from the *Yahoo* data breach in 2013, summarized by Stu Sjouwerman's *A Single Spear Phishing Click Caused The Yahoo Data Breach* blog, it is vital that those who work within the corporate system are given access only with the appropriate credentials to prove authority into the system and are using the systems appropriately. This could be enforced by having passwords changed every so often or disposable badges that expire after the work day.

The systems within the company can also be modified to only allow the necessary programs and accounts, preventing personal email logins and changing of security settings. This can also be further enforced by requiring staff not to be in rooms with sensitive machines while off duty.

The use of external devices or drives on company systems is a notable policy enforced by the United States military. As described by Luther Mitchell's warning on using usb devices on base computers, "The rules are clear: USB flash drive devices are not authorized to be connected to government computers and with good reason…USB flash drive devices pose a risk of loss and theft, and caution should be exercised when using them." (Mitchell 2013).

In the pharmacy that I currently work for, we make use of devising how long our sensitive information is kept and keeping reports if any incidents were to occur regardless of how trivial they may seem.

Not all information is necessary to keep for so many years. If a user of our company's service were to not log in for a set time or not have a need for the account, their information should be rightfully terminated as to prevent the backlogged information from being stolen. By only keeping what is necessary and relevant can we minimize the damages if an attack were to occur.

Now if an attack were to occur, it would be beneficial to keep an incident report. The reports as a way to keep a log of the vulnerabilities in the system and how we can address them. "...when staff report incidents, they are directly contributing to potentially preventing a future incident from happening again. It allows the organization to properly investigate and establish checks, procedures and implement risk controls in response to what has happened" (Incidentreport.net).

Prevention of unauthorized use of corporate systems begins with how the authorized users utilize the system and the steps they take to see that only the right hands access the sensitive information.

References

Adsero Security. (2023, January 10). *10 must have IT security policies for every organization*. Adsero Security. Retrieved January 29, 2023, from https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

Sjouwerman, S. (n.d.). *A single spear phishing click caused the Yahoo Data Breach*. Blog. Retrieved January 29, 2023, from https://blog.knowbe4.com/a-single-spear-phishing-click-caused-the-yahoo-data-breach

Mitchell, L. (n.d.). *Using USB devices on base computers big no-no*. Luke Air Force Base. Retrieved January 29, 2023, from https://www.luke.af.mil/News/Article-Display/Article/641390/using-usb-devices-on-base-computers-big-no-no/

What is incident reporting? What is Incident Reporting and why do you need it? (2022, December 7). Retrieved January 29, 2023, from https://www.incidentreport.net/whatisincidentreporting/