Joshua Morton's Proposition for Data Security and Recovery Policy

Joshua A. Morton

CYSE 300

Old Dominion University

As companies and organizations today become more and more dependent on technological systems and data storage, outward threats to sensitive information have become more commonplace as well. Companies now must not only face threats to their data but also face the halting of their entire operations if only one security breach leads to a site wide incursion and must react accordingly. To remedy the growing organizational and technological issues many companies have today it would be best to implement security and data protection policies for system users to follow. If were to be given the opportunity to create a organizational security policy I would take five main security issues into account, those being; the continued updating of operating systems, prevention of leaking of data from trusted users through monitoring, investing into higher forms of identity management, creating a system for understanding the number of assets in a system, and finally a plan for data recovery and response in the event of an attack.

I believe that before even implementing the security policy the organization in question should understand the amount of assets they have in their own system as many attacks may occur based on a single unidentified source, be it unauthorized laptop or mobile device, and as such this step is important so that during an attack the source may more precisely be pinpointed. When an accurate count of available assets is collected it is advisable to invest in certain systems to more accurately identify users, identification methods such certificate based authentication could be used to remedy the problem of unauthorized users remotely requesting secure data. Although a thorough system is added many organizations will still face the threat of secure information being leaked not from an outside source but from users inside the organization with authorized access to that data which may be remedied through the monitoring and auditing of accessed data from users so that administrators may see what data was accessed and what it was sent to to both better pinpoint who may be leaking data and what they head accessed. And lastly,

with the understanding of what assets a system has will give administrators find vulnerabilities in systems that may be running out of date operating systems or may not have the proper security measures which can prevent the use of exploits by those wishing to get into secure systems anonymously. For example, the WannaCry virus using an exploit based on outdated windows operating systems was able to grant full access to computers and if there had been a system

The methods of threat and vulnerability prevention may help to prevent a future attack but what would happen in the event of an attack? The answer would be to put into effect data recovery and crisis management plans. When an attack happens, having a plan is important to understand what data has been lost and this will help the organization better determine the financial loss. Having a plan also helps cybersecurity officials locate and eradicate the source of the attack or its entry containing that source and eradicating it.

Works Cited

Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*. https://www.amazon.com/Nist-Cybersecurity-Framework-Pocket-Guide/dp/1787780406

(2015). Cybersecurity: Setting the Rules for Responsible Global Cyber Behavior: Hearing before the Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy of the Committee on Foreign Relations, United States Senate, One Hundred Fourteenth Congress, First Session . .

Li, L., He, W., Da Xu, L., Ash, I. K., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Netalit. (2023, July 9). *Cyber Security Policy - Types of cybersecurity policies*. Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/cyber-security-policy-types-of-cybersecurity-policies/#:~:text=A%20cyber%20security%20policy%20provides,protect%20the%20company's%20sensitive%20information