Short Research Paper #2 - Cyber Policy

Brandon Zachary Pearson

Old Dominion University

CYSE-300 - INTRODUCTION TO CYBERSECURITY

Professor Malik A. Gladden

September 17, 2023

One of the significant concerns with modern companies is how they obtain user data. They collect a copious amount of data at times without informing the users. Additionally, users often overlook what data is being gathered by companies because they assume companies act in good faith. While there are companies that set the standard when it comes to implementing information security policies it is often that companies fall short in this area. In order to create a well-rounded information security policy, it should touch on the following policies: confidentiality, integrity, availability, data backups, and incident response.

A significant part of any information security policy is to go over the confidentiality efforts. Highlighting what efforts are going to be put forth to ensure the confidentiality of the data that is being collected. This can be seen in how a company expects employees to conduct themselves while handling private data, "employees must understand the organizational processes and business goals of their organizations, and provide protection along the entire course of the information flow." (Goodman, p. 37). Additionally, highlighting those who have access to data will keep the data private.

Integrity is another part that should be touched upon to inform the public on how they are planning to keep data safe. This could be through implementing encryption at various levels in order to add an extra layer of security. Encryption helps in many ways when it comes to maintaining the integrity of data. This is due to the data being encrypted which makes the information illegible to a human. In order to read the information, it would have to be decrypted which can take a long time. This makes the information that is being stored harder to gather without more effort being put in to read it. "Privacy preservation can be achieved by methods like cryptography, access control, and Homomorphic Encryption.". (Grandad, 2023). Another thing that should be highlighted when going over integrity is what the company has planned to

ensure the data hasn't been altered. Along with maintaining the data integrity establishing the availability policy allows users to know who has access to their data. Sharing what the data is being used for and if it is being shared with outside sources. One additional step that should be implemented is having a data backup policy. This ensures that there is a backup of all the information on hand if anything is to happen to datasets.

Incident response plans are an important thing to implement and establish for any company because it goes over how they will deal with breaches or any form of attack. This allows users to know what steps are going to be taken in order to combat and solve attacks that have taken place. This allows users to understand what companies are going to do in the event that their information has been breached. If they are going to release the information about it or how long they have till they let the public know of a breach.

Ultimately, it is important to implement information security policies in order to inform the public on how a company is going to operate. Companies that create a well-rounded information security policy can better address issues that come about. This creates a safer environment for the public and creates more trust that their information is being protected. No information policy is going to cover everything, but it is important to have since it establishes how the company handles information security.

References

Gadad, V. & Sowmyarani C. N. (2023). A Comprehensive Review of Privacy Preserving Data Publishing (PPDP) Algorithms for Multiple Sensitive Attributes (MSA). In C. Rabadão, L. Santos, & R. Costa (Eds.), *Information Security and Privacy in Smart Devices: Tools, Methods, and Applications* (pp. 142-193). IGI Global. https://doi-org.proxy.lib.odu.edu/10.4018/978-1-6684-5991-1.ch006

Goodman, Seymour, et al. Information Security : Policy, Processes, and Practices, Taylor & Francis Group, 2008. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/odu/detail.action?docID=435197.

Rowlands, I. (Ed.). (1997). *Understanding information policy*. Walter de Gruyter GmbH.

The 12 elements of an information security policy. Exabeam. (2023, February 27). https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

Yaofeng Tu, Jiahao Niu, Dezheng Wang, Hong Gao, Jin Xu, & Ke Hong. (2023). BDMasker: Dynamic Data Protection System for Open Big Data Environment. International Journal of Software & Informatics, 13(1), 87–115. https://doi-org.proxy.lib.odu.edu/10.21655/ijsi.1673-7288.00297