Brendo Pierce

October 1, 2023

CYSE525

Professor Demirel

Policy Analysis Two

In today's world, where technology plays an essential role in Corporate America, there are rules, regulations, and policies that have to be followed to keep companies and government organizations securely running. Furthermore, said companies that have cyberspace are filled with a variety of information and important data that is vital to the company, such as company secrets, staff personal information, and many more that are significant. To protect this information, a cybersecurity strategy called the Data Classification and Handling Policy has been implemented in most corporations, which illustrates how to categorize all data and ensure that it doesnt end up in the wrong hands. Although there are some stipulations around the Data Classification and Handling Policy, this policy is still integral in the realm of business operations. In this article, we will discuss the political implications that arise from the Data Classification and Handling Policy.

Even though the Data Classification and Handling Policy is beneficial to many companies that need to protect critical data, there are some implications regarding its redundancy with the other strategies and policies that are supposed to protect data as well. The "Principles for Responsible Data Handling" by the Internet Society, which dissects the overall responsibilities to handle all data in a liable manner, raises the question that some may have; "Why do we need to handle data 'responsibly' when there are often existing privacy and data protection rules?" (2019), and they answered with the following reasons: the innovation of technology moves faster than the creation of policies and strategies, and that just following rules

thoughtlessly promotes risk and compliance culture that miss the fundamental principles to data protection (2019).

Along with the political implications and the various doubts when it comes to the Data Classification and Handling Policy, there are also some challenges that the company faces and has to overcome for this policy to remain successful in its objective to classify and protect. In the National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE) Special Publication "Implementing Data Classification Practices", the potential challenges that have impeded or obstructed the process of data protection are illustrated. A few to mention are that some firms aren't using classifications that are consistent with those of their partners and suppliers because there are few compatible standards for data classification across diverse regulated industry sectors, and the amount of data being transmitted through various data centers, clouds, and other devices muddle the process of prolonging data inventories (2023). Also, NIST reiterated the fact that policies and regulations often change during the data lifecycle due to the constant technology change so that policies can be up to par with the technology of today (2023).

Due to the challenges associated with data classification and handling, NIST has implemented a certain approach for these challenges. In the NIST Data Classification Practices: Facilitating Data-Centric Security Management project description, they mention the zero-trust approach (or zero-trust architecture), which is a high-level approach that works under the premise that anyone trying to access business resources, including those inside the network, cannot be trusted (2021). Because of this architecture, many companies that have implemented this are successful when it comes to classifying and handling data.

Resources

Internet Society. (2019) *Policy Brief - Principles for Responsible Data Handling* https://www.internetsociety.org/wp-content/uploads/2019/06/Responsible-Data-Handling-Policy-Brief-EN.pdf

Newhouse, W; Souppaya, M; Kent, J; Sandlin, K; Scarfone, K. (2023) *NIST SPECIAL PUBLICATION 1800-39A Implementing Data Classification Practices* https://www.nccoe.nist.gov/sites/default/files/legacy-files/data-classification-project-description-draft.pdf

Scarfone, K; Souppaya, M. (2021) *DATA CLASSIFICATION PRACTICES Facilitating Data-Centric Security Management* https://www.nccoe.nist.gov/sites/default/files/2023-04/data-class-nist-sp-1800-39a-preliminary-draft.pdf