*Explain how Fortune 500 companies can use a data classification standard similar to the US Government and how/why it fits with the IT Security Policies already in place.*

**Chad Ballay**

**Week 1: Fortune 500 Companies – Data Classification Standards**

A core function of Information Security is to design, implement, and audit the procedures in place for data warehousing. The generation, enrichment, access, and storage of this data all depends on giving the access to those who need and denying those who shouldn’t have it. Intellectual property, trade secrets, customer data, vendor relationships, etc, etc…. Each of these have unique impact upon business operations and the lack of access to the right people can be just as impacting as the abundance of access to the incorrect people. (How to Select Data Classification Levels for Your Business, n.d.)

The first step should be to define a tiered system of classifying the data. A hierarchy of nesting buckets where if data is classified at *N* levels then all the details of how to treat the data at *N* and *N+1* levels get progressively looser. For instance, the US government uses the Top Secret, Secret, and Confidential tiers. Restrictions of Secret data are more constrained than the restrictions on Confidential but less constrained than Top Secret. (Classified Information In The United States, n.d.)

In the business world, the stakes are different, but the needs are still the same. Creating a limited number of tiers helps to ensure that consensus of what ranking data should receive can be quickly achieved. When you have more than a handful of tiers the splitting of hairs becomes an inefficient burden. Less is better. The primary delineation should be around business impact.

An example could be:

1. Company Confidential
2. Private
3. Sensitive
4. Public

**Company Confidential**

This would be the most restricted data. Things that have direct financial impact and regulatory compliance needs. *Examples: Project plans for acquisitions. Customer PII/HIPAA/CC numbers. Credentials. FERPA data. Lawyer communications. Full SSN.*

**Private**

This is still heavily restricted but often times the delineation could be the degree of regulatory compliance needed around the data itself. Security camera footage is extremely important but often no legal requirement around the data itself. *Examples: Building entry/exit records. Server access logs. Source Code. Trade Secrets.*

**Sensitive**

Data at this level should not be willingly disclosed but may often be compelled due to records request or inadvertent accidents. The key is that if this data is disclosed the impact will be negligible in single instances. *Examples: Employee manuals. Email conversations between coworkers. Employee userids.*

**Public**

Data at this level is often willing shared and made available. This is the data that you want to be shared or have no care of the impact if it is shared. It is either beneficial or has little chance of causing harm. *Examples: Technical blog cleared for release. Contact numbers for customer service.*

The underlying goal is that the levels have to be unambiguous as to what belongs into which tier. Once the tiers have been identified then the access controls around the lifecycle of the data should be crafted. Who owns the data creation? How is access granted? When can the data be deleted? How redundant should the data be stored? Etc, etc…. (Sotnikov, n.d.)

At the heart of it the company’s business goals will dictate the quality of care the tiers receive. Enumerating the tiers and providing business-oriented justifications to the tiers will allow for the prioritization of how much resources can be allocated in securing the data in a specific tier. The guidance of an effective Data Classification Standard is invaluable.

# Works Cited

*Classified Information In The United States*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Classified\_information\_in\_the\_United\_States

*How to Select Data Classification Levels for Your Business*. (n.d.). Retrieved from GetApp: https://lab.getapp.com/data-classification-levels/

Sotnikov, I. (n.d.). *How to Build an Effective Data Classification Policy for Better Information Security*. Retrieved from Netwrix Blog: https://blog.netwrix.com/2018/05/31/how-to-build-an-effective-data-classification-policy-for-better-information-security/