The number of records that were compromised often measures the severity a data breach. Organizations may consistently monitor for these leakages and provide alerts on certain criteria. Specifying alert criteria can help a company better utilize its time and resources. Providing data models for specific domains to measure the severity of leakages can aid in this process. The severity can be based on many factors and should consider how much an attacker can infer about a subject from the leaked data. This work evaluates different similarity and diversity metrics in coordination Leakage Severity (L-Severity). Often data may come from many sources and is displayed on desktop applications or browsers. We will design a data model at the application level to present a way to measure severity from multiple containers.