FORTRA

**CASE STUDY** (Boldon James)

# Enhancing Data Governance: Eliminating The Known Unknown

## Using Data Classification to Ensure Your Sensitive Data is Kept Secure

When discussing data governance tools, it's no secret the topic of false positives is seen as one of the biggest downfalls. False positives occur when an event is triggered by the data governance policy in error, for example, a combination of numbers could be identified as a credit card number, or a reference number. This means that data can be quarantined unnecessarily, stopping people going about their daily business. Data governance tools' job is to enforce appropriate handling of data throughout its lifecycle based on the sensitivity of the data. This includes data loss, who is able to access certain data, where data is stored, how it is shared and what level of protection is required.

### The Lesser Known Problem

The challenge associated with false positives is widely known, understood and easy to quantify. The opposite challenge is rarely discussed, and proves to be the most challenging when it comes to protecting your sensitive data; false negatives. A false negative is essentially when a data governance tool fails to detect occurrences of data leakage it was intended to capture; usually a scenario in which the appropriate handling rules were not applied, and data may have been lost because the data governance tools did not fully understand the sensitivity of its content. This is a more significant challenge, as it directly leads to the loss of sensitive data, and by nature is virtually impossible to fully quantify.

The main purpose of data governance tools is to prevent data loss, but in the case of false negatives, the heart of the issue is sensitive data which has been lost. Not only has this data been lost from the organisation, but the data governance solution hasn't correctly detected that it should be stopping it from leaving.

> "50% of ISF Benchmark respondents do not review policy violations to help minimise false negatives and false positives."
>
> *Information Security Forum Benchmark analysis, 2018*

One of the biggest complications here is how can you quantify these losses? You're losing data, but the data governance tools aren't able to show you just how much. If you can't quantify the risk to the board, they are unlikely to react, however, valuable data is very much at stake.

## Using Classification To Eliminate False Negatives And Positives

The issues of false negatives, and positives, are common in the sense that anyone using a data governance solution will come across these at some point in the product's lifespan. Remediating false positives involves tweaking the current company policy, often resulting in one area being fixed, only for another to go wrong. This is often an ongoing problem that is never completely solved. Less commonly addressed are the false negatives. Preventing these is more of a complex task when solely using a data governance tool, as the only way of being able to act is if the cause of the data loss is very apparent.

Using data classification is an easy way to solve data governance false positives and negatives. Using classification alongside data governance tools means that instead of the data governance tool having to look through a long list of policy variables to determine what to do with the data, the tool just has to look at the metadata that is added to the document by the classification solution. The metadata is able to accurately show whether the document contains "confidential", or "sensitive" data, and should be blocked rom leaving the organisation, to enable false positives and negatives to be eliminated.

By using metadata to drive your data governance tool, policies can be focused on specific areas to then reduce false positives and negatives. Generally, rule sets in data governance tools will be set to search for information such as PII, or key terms such as "acquisition" within the document. Rules like these allow the data governance tool to make an easy decision based on simple, straightforward, terms.

However, often you will find there is nuanced information that doesn't fit directly into the policy rules, but is still highly confidential. If the toolset can then look for a classification tag within the metadata, as opposed to just a rule variable, this information too can be correctly identified and protected. This eradicates the risk of the data governance tool not being able to apply the simple rule set, resulting in data loss.

Your users are one of your organisation's biggest security assets. Users are more reliable at classifying the sensitivity of a document, knowing the context of what is contained, rather than a tool simply looking for a specific set, matching data to the rules it is programmed to identify. By letting users apply this level of granularity to documents through classification, you have far greater control of the data not only stored within your organisation, but what can and cannot leave the organisation.

To find out more about how your organisation can use Boldon James Classifier to boost the performance of your data governance tools, **get in touch today**.

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.