

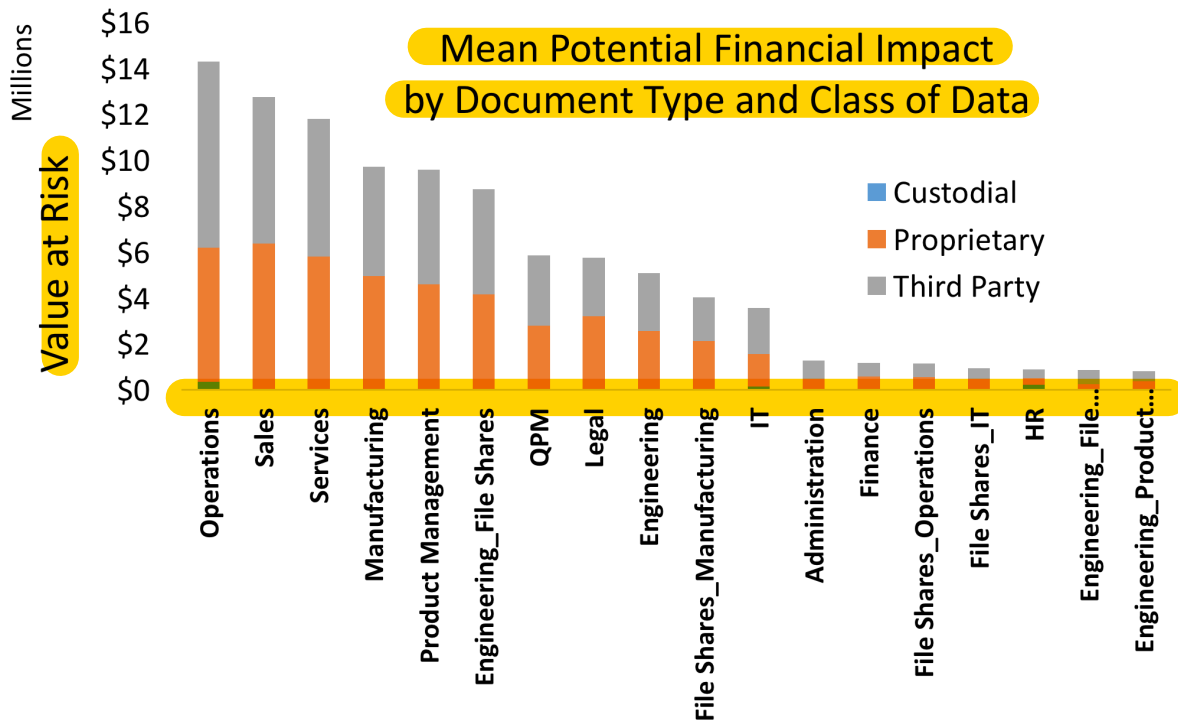
[Home](#)[Solutions](#)[Risk Quantification](#)[Services](#)[Blog](#)[Company](#)[Home](#) / [Our Quantitative Approach](#)

# Our Quantitative Approach

Our statistical models are built using well-defined methods in a rigorous approach. They are credible loss forecasting models based on empirical data. They are deterministic models that ensure compliance.

## Rigorous Analysis

We provide credible loss forecasting based on empirical data and deterministic models (regression). Our method involves rigorous analysis of every department, document type and type of attack. We perform data cleaning, filtering, pre-processing and transformations.



## Robust Verifiable Models

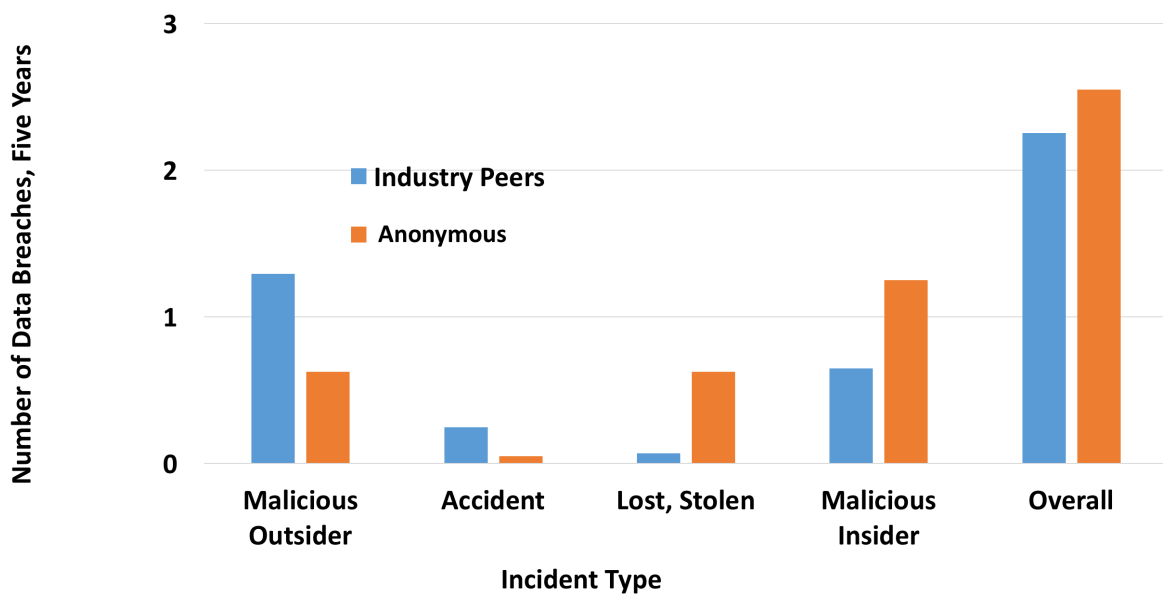
We validated our models under the federal bank regulator's guidelines, SR11-7.

Our model testing includes sensitivity analysis, robustness testing, p-value and r-squared, jackknife/bootstrap, cross-validation/independent validation set, stability and extreme value testing.

# Defensible Calculations

The statistical robustness tracks and tests that we've done to make sure that the model's forecasts are solid and grounded in the historical data to meet the federal bank regulator's guidelines, SR11-7.

We test the model using other cyber incident data that was not used in building the model. We can test the model's forecast and predictions to see if they're accurate.



© Copyright 2012 - 2018 VivoSecurity Inc, Los Altos California

Contact: ask@info.vivosecurity.com, (650) 822-8486

