CASE STUDY

RiskLens Shows Financial Institution Its Risk Exposure in Moving to Office 365

Challenge

With many other organizations moving to Office365, the Information Security team wanted to know if the additional features like more robust patching, email blocking and better DLP, would be worth the additional cost to the organization given their current controls environment.

Solution

Using RiskLens, the team analyzed the risk exposure in financial terms of moving to O365 for the organization.

Results

For the first time, Information Security could effectively discuss and communicate risk exposure in business terms rather just red, amber or green. This gave executive management the opportunity to see first hand how risk quantification could help their organization.

The Challenge

A financial services institution with $10B in total assets was trying to determine if a move to Office 365 from their internally hosted Exchange Server made sense for the organization. They knew they could save considerably on hardware and software maintenance and security costs. But they worried that their customer records would be more exposed to a data breach if they moved to the cloud-hosted O365.

The Information Security team advocated that the move to O365 would provide a much more secure environment than what they currently were able to provide self-hosted. Executive management trusted the team but still wanted reassurance. But the only method InfoSec had for determining risk was an Inherent and Residual Risk “calculation” that helped them choose a red-amber-green rating. Analysts needed a new way to communicate risk that was consumable by business stakeholders, in other words, in dollars and cents.

The Solution

The InfoSec team turned to the RiskLens platform. It combines risk-scenario scoping and data collection with an analytics engine powered by Factor Analysis of Information Risk (FAIR), an industry-standard model for the quantification of information security risk.

Analysts used the scoping capability within RiskLens to rapidly determine what data points were necessary for the analysis, effectively reducing their work load by removing research into data that did not ultimately support quantifying risk.

Using the RiskLens platform’s structured workshop questions on key risk factors, analysts collected data such as the historical number of confirmed breaches, both malicious and in error. With real-life examples in hand, the team was able to accurately estimate the financial impact of the actions the organization would take should a breach occur.

They were able to review all of the controls they had in place to prevent breaches—for example, their current patching process, email filtering capabilities and encryption abilities—as a baseline to compare against the likely improved security available from O365. With less time invested in RiskLens than previous methods, the team was able to efficiently produce both high level reporting and detailed results that quantified in financial terms the change in the organization’s risk of a breach in moving to Outlook 365.

The report showed the effect of moving to Office 365 both in aggregate loss exposure and individual categories such as costs of incident response, fines & judgments and reputation damage.

With RiskLens risk quantification, this institution saw current and future risk clearly in financial terms for the first time.

Inevitably, estimates used to calculate risk have a degree of uncertainty associated with them. However, the results of a RiskLens analysis are always distributions based on probabilities (see Fig.1 below) to account for uncertainty.

Key Benefits

The RiskLens platform allowed the Information Security team to rapidly quantify the probable loss exposure of a move to O365 in financial terms - a more meaningful measurement for business decision-making. Once the current state analysis of loss exposure was complete, the future state was easily analyzed using the same process, while also reducing the subjectivity of results. The institution also discovered they could leverage RiskLens to aggregate the exposure associated with each actor, gaining a total risk perspective based upon threat actor. In doing so, they found that the threat actor type that posted the most risk was employees acting in error.

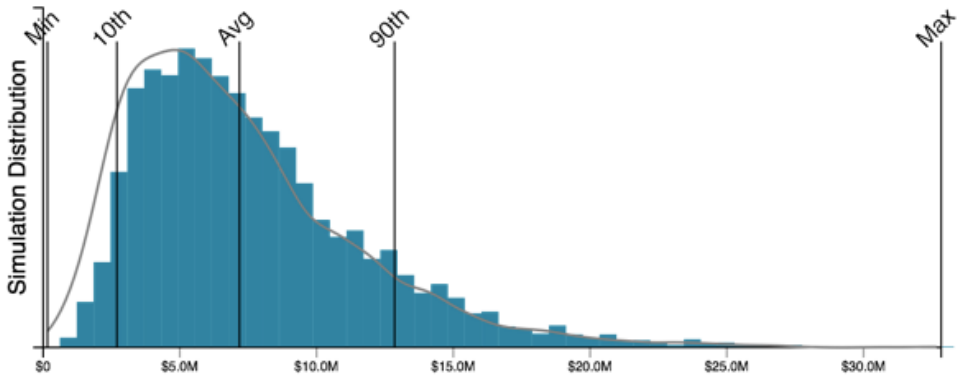

Fig. 1 - Aggregate Loss Exposure

The current state loss exposure (average) is $7.2M, annualized. Moving to Office 365 would cost an additional $100K annually in license fees. The future state shows an annual average risk reduction of $4M, even accounting for increased fees. With a quantified understanding of the impact of a breach of sensitive customer records, executive management confirmed it would be a smart business decision to move to the Office 365 suite hosted in the cloud.

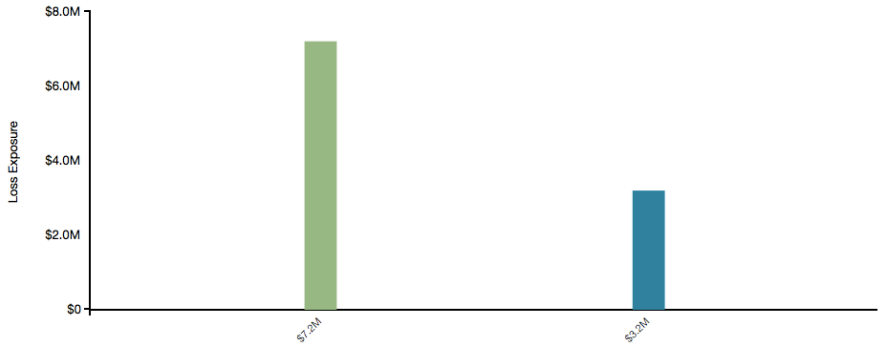

Fig. 2 - Average Annualized risk reduction