CASE STUDY

# Large Financial Firm Justifies Security Investments with Risk Quantification

**Challenges**

With business stakeholders evaluating many opportunities to create/protect value; security management struggled to effectively communicate the value of security initiatives and projects in business terms.

**Solution**

Using RiskLens, security management created a cost/benefit analysis showing the current-state loss exposure and the forecasted reduced level if a security investment in a leading vendor service was implemented.

**Results**

- Analysis report on current level of loss exposure associated with malware incidents;
- Analysis report showing the forecasted reduction in exposure with implemented vendor service;
- RiskLens' Comparison Report enabled security management to communicate the business value the proposed security initiative.

## The Challenge

A leading financial services firm with $2B in revenue and over 3,000 employee workstations has tracked increases in the number of malware incidents over the past year. They have identified a leading vendor service that they believe can help them address this growing issue. However, security management is often challenged by the business when justifying the value of larger security investments using current risk ratings based on a qualitative scale of High, Medium, Low or 1-1000.

The methods of communicating risk within cyber security haven't improved significantly over the last decade. The predominant use of qualitative scales and ratings have limited value in enabling well-informed business decisions. Recently more gradual scales such as 1-1000 are being positioned as sophisticated and data driven. The underlying limitation is that those solutions still lack business context - **what does 478 mean to business stakeholders?** Security needs to start communicating cyber security risk in financial terms (i.e. dollars and cents).

## The Solution

RiskLens' platform combines an intuitive workflow process for scoping and data collection with a sophisticated analytics engine based on Factor Analysis of Information Risk (FAIR), an industry standard for the quantification of information security risk.

The analysis collected data through structured workshop questions on key risk factors including number of historical malware infections, level of vulnerability across workstations, and resources required to resolve incidents. The analysis also considered secondary events such as customer data that may be exfiltrated which would result in additional liability and losses. The firm was able to efficiently produce both high-level reporting and detailed analyst results that quantified the current level of loss exposure (risk) associated with malware incidents for the organization.

| | |
|---|---|
| Maximum | $59.5M |
| 90th % | $17.4M |
| Average | $6.6M |
| 10th % | $107K |
| Minimum | $19K |

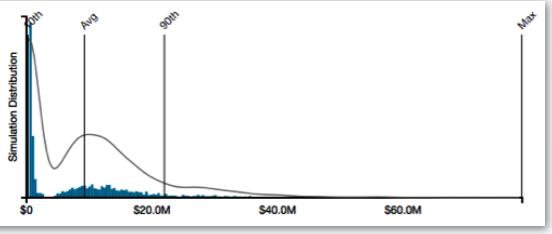


fig. 1 - Current State Loss Exposure (Avg. $6.6M)

with the current state analysis completed. The firm leveraged the versioning capability within RiskLens' platform to rapidly produce a secondary analysis with all existing data points carried over. In this secondary analysis they identified the key factors that the malware protection service would improve and estimated its effectiveness (a reduction in threat event frequency). Inevitably the estimates related to improvements have a degree of uncertainty associated with them. However, like all data input into the analysis, distributions allow the organization to account for uncertainty. In less than an hour the firm produced a second report forecasting the reduction of loss exposure with the implementation of the recommended vendor service.

RiskLens provides powerful built-in comparative reporting that allowed the firm to incorporate the results of both analysis into a single report. This report clearly illustrated the change in loss exposure in both visual and data-focused tables.

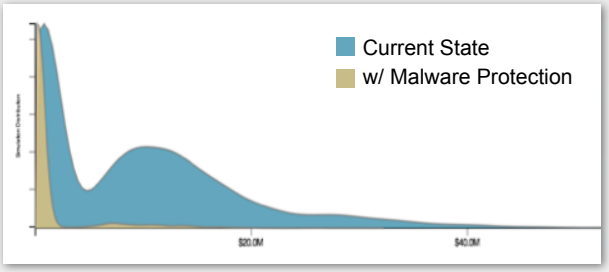


fig. 2 - Comparison (Avg. $6.6M reduced to $1.2M)

## Key Benefits

RiskLens' platform allowed the security risk team to rapidly quantify the current-state loss exposure in financial terms. This was a first for information security and they found the structured analysis process improved the consistency of analyses while also reducing the subjectivity of analysts.

The firm further discovered that by leveraging RiskLens' versioning and comparative reporting that they could now build risk-based business cases to improve communication and decision-making.

Current state loss exposure (average) was $6.6M annualized. The malware protection service had an estimated cost of approximately $500K per year. With the mitigation investment, the forecasted loss exposure was reduced to $1.2M - A clear business case for the CISO. The proposed security initiative was favorably supported and approved by the business.

**RiskLens**

850 E Spokane Falls Blvd, Ste 270
Spokane, WA, USA 99202

11911 Freedom Drive, Ste 850
Reston, VA, USA 20147

**Toll Free**: 866.936.0191
**Web:** www.RiskLens.com

## About RiskLens

RiskLens is the premier provider of cyber risk management software. RiskLens empowers large enterprises and government organizations to manage cyber risk from the business perspective by quantifying it in dollars and cents.
Our customers leverage RiskLens to understand their cyber risk exposure in financial terms, prioritize their risk mitigation, measure the ROI of their security investments, and optimize their cyber insurance coverage.

RiskLens is the only cyber risk management software purpose-built on FAIR, the only international standard Value at Risk (VaR) model for cyber security and operational risk.