CASE STUDY

Manufacturing Company CISO Confidently Justifies IP Protection Project

RiskLens

Challenge

A CISO had spent heavily on controls to protect the company's intellectual property—then management wanted to see proof, in dollars and cents, that the risk reduction justified the project.

Solution

Using RiskLens, analysts modeled historic and current data to produce a quantified estimation of risk, before and after the controls.

Results

The CISO presented management with a cost/benefit analysis that conclusively justified the project, in exactly the financial terms that management demanded.

The Challenge

The CISO at a global manufacturing company with $50 billion in revenue faced an all-too-common problem: intellectual property (IP), critical to their success and position in their market, was scattered throughout the organization, exposing them to grave occurrences of IP exfiltration.

To combat this exposure, the CISO was able to convey to executive management the value proposition of creating a centralized repository, with an abundance of security controls that would ultimately create a virtual data vault.

Over the next year, the company spent heavily to identify and consolidate all the IP, segment it from the network and protect it with a data loss prevention (DLP) solution.

Management congratulated the CISO on a job well done.

So far so good.

But even at a $50 billion company, budgets get tightened and priorities change. Management came back to the CISO and required a *retroactive* justification for the initiative's achieved risk reduction; in other words, to measure risk both before and after the controls.

The CISO was in a spot. The problems: How to find data on historic and current risk—and then how to assess that risk. The CISO's only existing tools produced qualitative high/medium/low risk ratings. The C-suite was going to need more than that to justify the initiative; they were going to need to see risk in dollar figures.

The CISO reached out to RiskLens for a crash course in understanding risk quantification and the process involved to quantify information risk in financial terms.

The Solution

The RiskLens platform combines two features to solve the CISO's problems: a process for scoping and collecting data plus a sophisticated analytics engine based on Factor Analysis of Information Risk (FAIR), an industry standard for the quantification of information security risk.

Using the platform, analysts were able to first identify the data points needed to perform the analysis. A FAIR analysis estimates risk (or loss exposure) based on the probable magnitude of loss and the probable frequency of loss events (for this company, the likely events would be an exfiltration of IP by cyber criminals or malicious, privileged insiders).

Guided by the platform's structured workshop questions, analysts were able to fairly quickly identify dollar values for various forms of potential loss (for instance, cost of responding to a cyber event), based on the company's good record-keeping.

"The RiskLens platform afforded the CISO the ability to rapidly quantify current and historic loss exposure (risk) in financial terms."

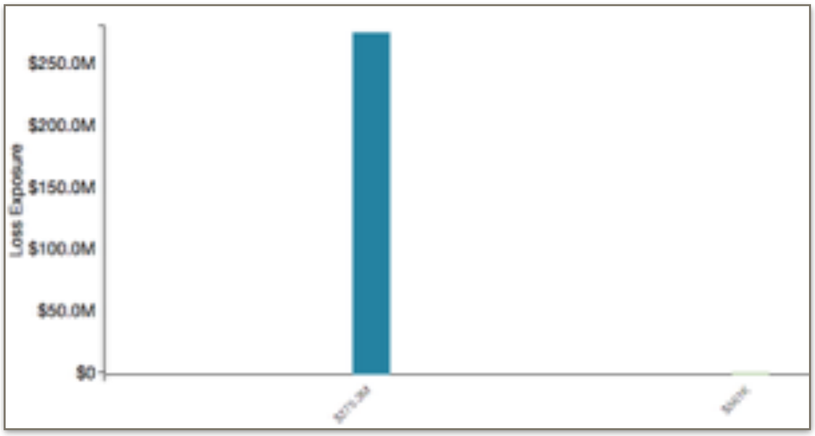
But the company had little data to go on regarding loss event frequency. RiskLens leveraged their measurement concepts and data gathering techniques to identify malicious activity seen on their network, combined with industry-wide data, and an assessment of security controls in place, to give a complete picture, both before and after the implementation of the virtual vault.

The resulting report showed both the before and after probable loss exposure quantified in dollars. Specifically, results were shown in annualized terms, and as distributions to account for the level of variance in experiences and degree of uncertainty associated with forecasting future events. The distributions were generated by running a vast number of potential scenarios through a Monte Carlo engine.

Results & Benefits

The RiskLens platform afforded the CISO the ability to rapidly quantify current and historic loss exposure (risk) in financial terms - the most meaningful measurement for business decision-making.

The organization went from an average annualized loss exposure of $275 million without the virtual vault in place, to $561,000 with the virtual vault in place, reducing the annualized loss exposure by 99%. Backed with this information, the CISO was able to confidently justify his decision to executive management.


Loss Exposure
$250.0M
$200.0M
$150.0M
$100.0M
$50.0M
$0
$275.3M
$561K