☎ 866.936.0191
www.risklens.com

CASE STUDY

Building a Business Case for Enterprise Asset Management for a Defense Contractor

Justifying budget is one of the key benefits of a quantitative cyber risk management program. This case study shows how one organization leveraged RiskLens for a budget win in the complex sphere of enterprise asset management for technology.

It should go without saying that an organization can't defend what it doesn't know it has. Should, but does not, as evidenced by the number of organizations that struggle to fully implement effective enterprise asset management solutions today. What's the underlying problem?

No one factor can be said to have caused the failures of technology asset management we see today. It's a confluence of these and other developments:

- The rapid growth of mobile device ownership
- The proliferation of workplace software products that require license tracking
- An increasingly interconnected global marketplace and supply chain that requires wide geographic distribution of assets
- The increased complexity and siloing of knowledge in today's organizations

The Challenge

Understanding how critical asset management is to the sustainable success of an organization, many IT Operations, Cyber Risk, and Information Security professionals find themselves arguing for comprehensive asset management but struggling to effectively communicate the return on the required investment in people, process, and technology.

That's exactly where a team at a leading civil/defense/cybersecurity contractor found themselves recently — struggling to articulate a business case for asset management. The team was understandably frustrated. The value of asset management seems so obvious, and its importance so great, yet they hadn't convinced the folks who control the purse strings to make the investment. They turned to the RiskLens platform leveraging the FAIR methodology to help them view the problem in a different way.

Challenge
Remediation teams were spending hours tracking down asset owners each time a vulnerability scan was issued.

Instead of talking about the benefits of asset management in bullet points and verbal descriptions of capabilities, they wanted to show business leaders how a lack of asset management was currently impacting their bottom line. And they wanted to do it in the language those business leaders speak — dollars and cents.

Through interviews conducted by expert FAIR™ analysts from RiskLens, one crystal-clear example of a loss event caused by poor asset management emerged: Each month vulnerability scan results were distributed from a central security function to seven remediation teams across different lines of business, each expected to remediate identified vulnerabilities on their hosts within a short time frame.

But there was often a problem: vulnerabilities identified on hosts no one knew anything about. Remediation teams were spending hours and hours tracking down asset owners and documentation each time a vulnerability scan was issued. They were slowly adding information to their own databases and spreadsheets, but unable to benefit from a centralized, up-to-date, comprehensively and collaboratively populated asset management solution.

The Solution

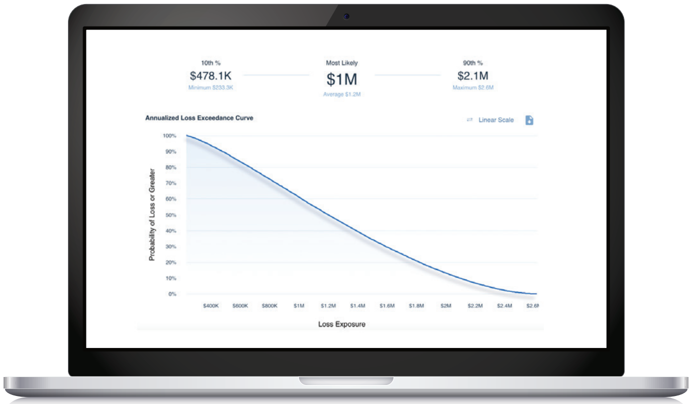
Using RiskLens, the team analyzed the losses associated with a lack of asset management impacting the efficiency of the vulnerability patching process. This loss event was occurring each time a new vulnerability scan was issued. Since that was a regular process that occurred every two weeks, it made estimating Loss Event Frequency simple: 26 times a year is the minimum, maximum, and most likely value.

For Loss Magnitude, the team interviewed leaders from two of the seven impacted teams, obtaining estimates of how many person-hours were being spent tracking down poorly documented hosts each time a scan report was issued (16 to 120, with a most likely value of 60 shaped with low confidence since it varied widely from report to report) and the average loaded hourly wage of the team members tracking down and remediating these vulnerabilities ($80 to $120, with a most likely value of $80, again with low confidence to reflect similar probability across all parts of that range.)

Solution

Analysts ran thousands of simulations on the RiskLens Platform, with data inputs derived through the FAIR Model.

Thousands of simulations were conducted based on these estimates. In each simulation, the amount of loss experienced over a one-year period was determined by randomly sampling a number of loss events (26) and an amount of loss per event ($8,960 to $100,800, with a most likely value of $33,600 with low confidence.) Summarizing the total amount of loss experienced in each simulation we can draw inferences about how much loss we are likely to experience over the next year from this scenario.



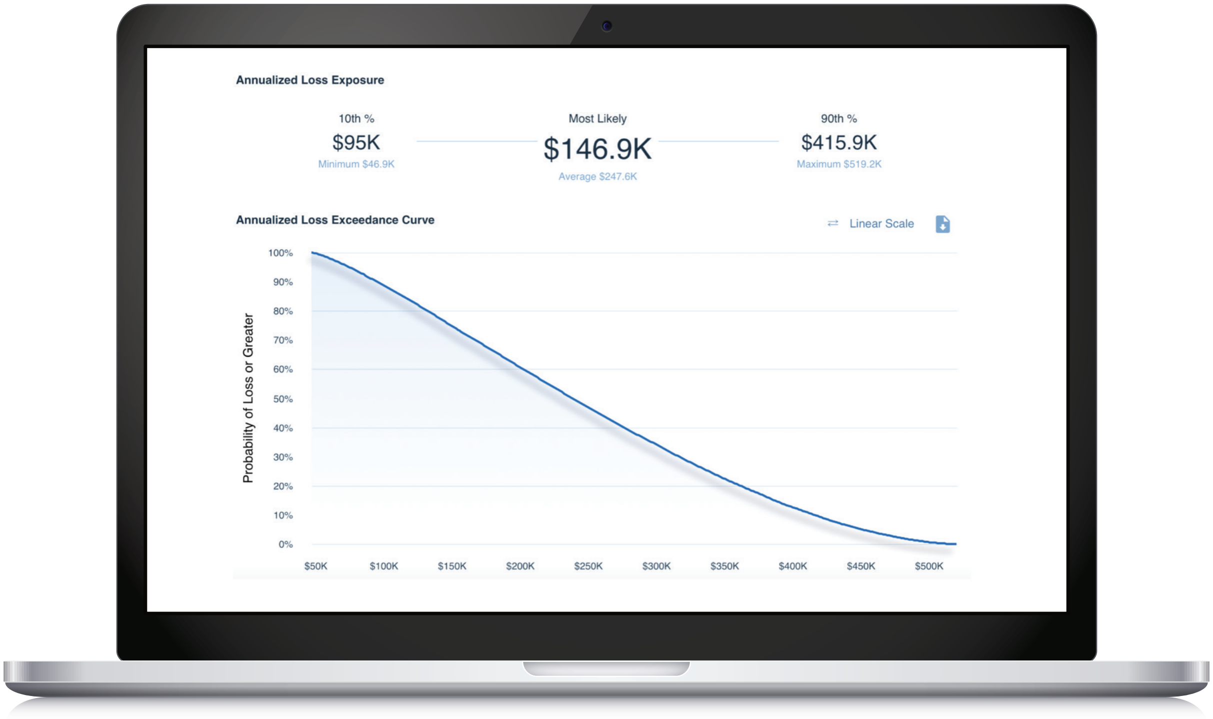
Results & Benefits

As shown in the image above summarizing the results of the simulations, the most likely amount of loss from this scenario over the next year is around $1M, with a 10% chance of $2.1M-$2.6M lost in wages paid for unnecessary time spent tracking down assets. That's far more in operational losses in one year than the cost of an enterprise asset management solution.

Finally they had information that would be immediately clear to their, thus far, unconvinced decision-makers. The team estimated that with an enterprise asset management solution they could eventually reduce the time spent tracking down unknown hosts by as much as 80%. Given this estimate, the team ran a new set of simulations showing annualized loss from this scenario in the future, post-implementation.

Results

The team estimated that with an enterprise asset management solution, they could reduce by 80% the time spent tracking down unknown hosts.



But, as the team was quick to point out, this is just one piece of a much larger puzzle. Implementing an asset management solution will similarly reduce the loss exposure to a number of other scenarios, including:

- Unexpected payments after periodic software license audits/true-ups
- Higher tax burden due to inaccurate asset depreciation in financial statements
- Loss due to confidentiality breaches caused by unpatched vulnerabilities or overlooked assets

Any or all of the scenarios above could be similarly analyzed by making current state estimates of Loss Event Frequency and Loss Magnitude, allowing the team to add more and more line items to their business case for comprehensive asset management. This exercise perfectly demonstrates the flexibility of RiskLens, built on the FAIR model, and the ease with which it can be applied to operational risk scenarios and questions of business process efficiency.

With the clarity and defensibility provided by quantitative risk analysis using RiskLens, the team had complete confidence to successfully speak the language of the business leaders they needed to convince, talking in terms of real dollar impacts to the organization's bottom line.

Let's Talk About Your Cyber Risk in Business Terms

RiskLens is leading a revolution in the way cyber risk is assessed, measured and managed by bringing to market a Software as a Service solution that makes cyber risk quantification a reality.

We help organizations translate cyber risk from the technical into the economic language of business.

Schedule a demo.

☎ 866.936.0191
🌐 www.risklens.com