KOVRR

You Can't Prioritize What You Can't Measure

Budget Planning & Investment Prioritization | Case Study

Overview of the Company

A large retail company with over $3.5 billion USD with a $24 million cybersecurity budget. The company operates globally with 31 subsidiaries. The main cybersecurity team is located in the United States with additional information security professionals dispersed geographically to support operations. The company uses the CIS framework.

Problem

The company wanted to build out the annual budget and prioritize initiatives in which cyber investments matched business objectives and risk appetite. Due to internal company initiatives, it was important to connect cyber budgets to overall business unit budgets in a data-driven way. They were looking to run several simulations of the company with varying suggestions of security control implementation levels based on a set of 30 projects identified as "crucial" for operation. With the current budget, it was clear that a smaller subset of projects could be implemented with preference for specific business units.

Solution

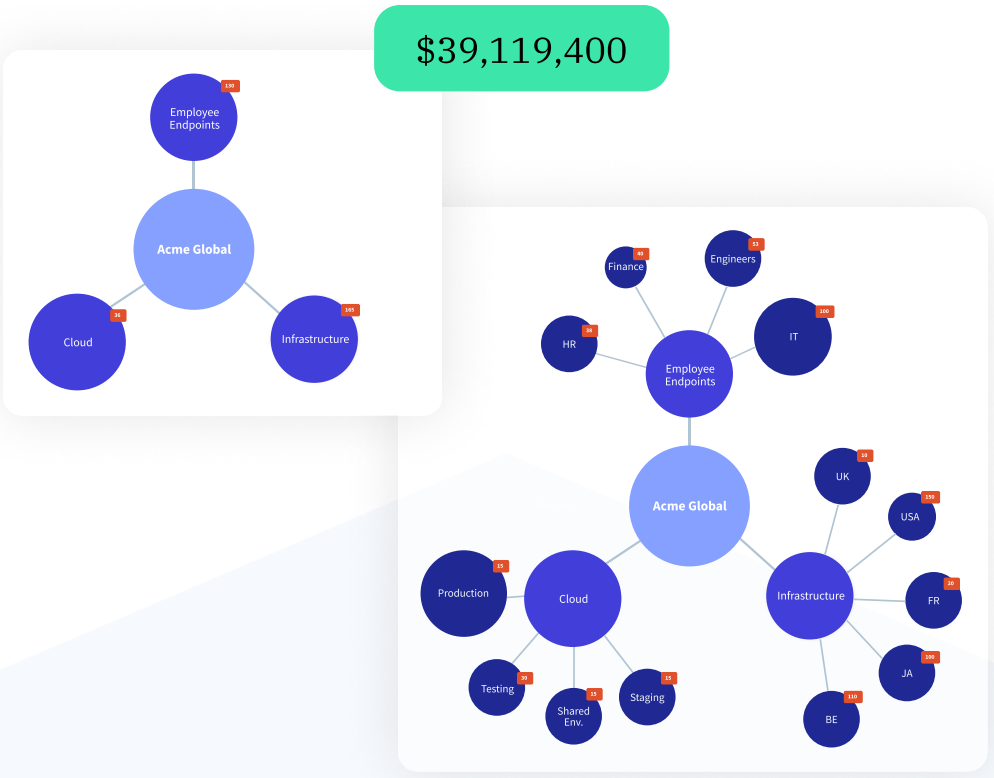
The goal of the company was to first understand the overall exposure on a group level and then to dive deeper into their overall exposure by breaking down the groups into smaller entities.

The company began the process by running a cyber risk quantification on the entire group. This was done using Kovrr's Cyber-Sphere and internal data integrations with Microsoft & ServiceNow.

The first run was split by business units and provided them insight into which business unit had the highest exposure. This was done to examine their initial assumptions and validate or change preference of business units.

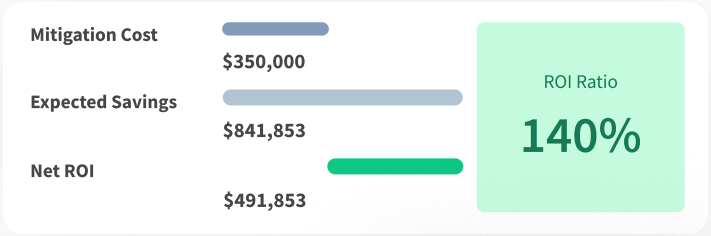
Next, the group ran each business unit separately. For each business unit, the retail group reran the quantification after changing the assumptions about the maturity of security controls based on the planned projects.

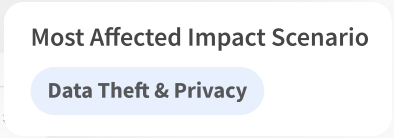
Next they evaluated the ROI of each change using the ROI calculator. After running a total of 76 simulations, the company was able to identify the projects that would significantly lower the company's financial exposure.

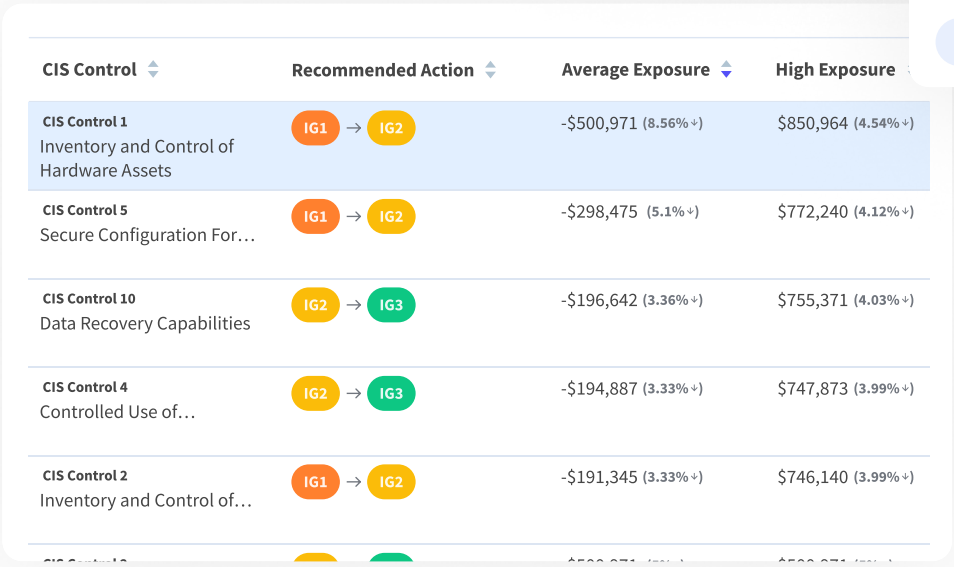


Outcome

The company prioritized 12 major projects. The projected ROI for the projects ranged from 17% to 165%. The retail group presented the associated financial exposures of the first simulation alongside simulations with control upgrades. They also calculated ROI by mapping project costs and benefits of implementation to the financial exposure associated with each security control. Using the ROI quantifications, allowed the CISO to communicate the risk to both the CIO and CFO in financial terms which fit their operational objectives and avoid the allocation of resources to projects that did not yield enough reduction in overall cyber exposure of the business. The CISOs ability to clearly show prioritization due to financial exposure helped him bring stakeholders on board to approve the budget.







CIS Control	Recommended Action	Average Exposure	High Exposure
CIS Control 1 Inventory and Control of Hardware Assets	IG1 → IG2	-$500,971 (8.56%↓)	$850,964 (4.54%↓)
CIS Control 5 Secure Configuration For…	IG1 → IG2	-$298,475 (5.1%↓)	$772,240 (4.12%↓)
CIS Control 10 Data Recovery Capabilities	IG2 → IG3	-$196,642 (3.36%↓)	$755,371 (4.03%↓)
CIS Control 4 Controlled Use of…	IG2 → IG3	-$194,887 (3.33%↓)	$747,873 (3.99%↓)
CIS Control 2 Inventory and Control of…	IG1 → IG2	-$191,345 (3.33%↓)	$746,140 (3.99%↓)

About KOVRR

Kovrr financially quantifies cyber risk on demand. Our technology enables decision makers to seamlessly drive actionable cyber risk management decisions.

contact@kovrr.com www.kovrr.com www.kovrr.com