KOVRR
Cyber Decisions. Financially Quantified.

CASE STUDY

Quick, Quantified Cyber Risk Metrics Help Bystronic's CISO Take Action

Cutting Cyber Risk Exposure in Half With Kovrr's CRQ Platform

www.kovrr.com

Overview of Company

Bystronic is a leading global technology company providing solutions for sheet metal processing. Since its founding in 1964, the organization has grown rapidly, with its portfolio now including laser cutting systems, press brakes, and software tools. With headquarters in Switzerland, the company has additional development and production sites located in Germany, Italy, China, and the USA. In 2021, Bystronic became listed on the SIX Swiss Exchange and, in 2023, had a net revenue of $1.07 billion.

The Problem

CISO and Head of IT Infrastructure, Simon Schlumpf, began his tenure at Bystronic a little over two years ago. In his previous role, Schlumpf had had the opportunity to build the information technology and cyber risk management program from the ground up, investing significant time and resources into assessing the organization's infrastructure, determining the various scenarios likely to occur, and manually calculating the potential financial impact should those scenarios take place.

While the CISO was pleased with the results gleaned from his in-house quantification, after he arrived at Bystronic, he understood that he did not have the same time to reproduce this effective yet resource-consuming process. Instead, he needed to assess the company's cyber risk exposure quickly and get to work on a new cybersecurity roadmap.

Moreover, senior stakeholders, who had historically relied on peer benchmarks to evaluate the organization's cybersecurity posture, now sought more specific, data-driven insights tailored to Bystronic's unique risk profile, necessitating a faster, more precise approach to quantifying cyber risk.

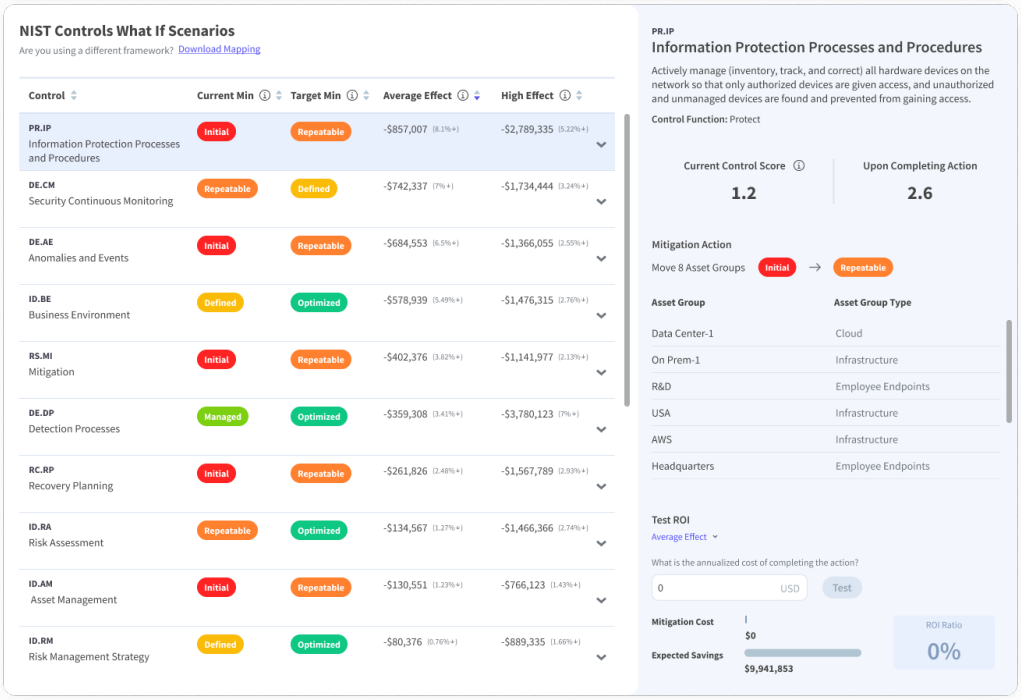
The Solution

Around the same time that Schlumpf started, Bystronic successfully completed an ISO 27001 audit, giving the CISO an accurate, tailored, and in-depth measure of the organization’s cybersecurity maturity. However, while these maturity levels provided a valuable basis for crafting a cybersecurity strategy, he decided he needed to augment the results by quantifying them to glean a more practical understanding of what they meant from a business perspective.

Consequently, Schlumpf searched for an on-demand cyber risk quantification (CRQ) solution that could provide him with these objective insights and soon found Kovrr. After an initial demo of the platform, the CISO decided to move forward. Within only a few days, he was taken through the onboarding process, had his Cyber-Sphere - Kovrr’s proprietary framework that allows companies to capture the complexities of their organizational setups and assets - created, ISO cybersecurity maturity levels mapped, and received his CRQ insights.

> *"One of the most intriguing features of Kovrr was the swiftness of the onboarding process… I knew I needed something very quickly, and with Kovrr, I received my actual results in days. So it was really quick, which helped kickstart a lot of my discussions as a CISO."*

Kovrr's Cyber-Sphere CRQ methodology also rendered it relatively easy for Schlumpf to model diverse business units. For instance, Kovrr's approach allowed him to compare the risks posed across these different subsidiaries despite their operational differences. He also used the Cyber-Sphere to separate these units according to their geographical zones, making it straightforward to assess cyber risk variations according to location.



Kovrr's 'What-If' scenarios highlight the average and high financial effects security control upgrades would have on an organization's overall exposure.

Once the initial quantification was complete, the CISO and Head of IT Infrastructure started exploring the platform, finding a particular value in the "Risk Management" component of the dashboard, which allows him to evaluate multiple "What-If" scenarios and the ROI of various security control upgrades, new solution implementations, or structural changes. With these insights, Schlumpf was able to make the ongoing data-driven decisions necessary for building a risk-based cyber risk management strategy.

The Outcome

Kovrr's quick time-to-value enabled Schlumpf to assess Bystronic's exposure rapidly, providing him with the necessary information to help shape his new cybersecurity roadmap. **Within two years, he has been able to cut this cyber exposure by half.** The risk forecasts helped him to discern which initiatives to prioritize, allowing him and his team to tackle those "low-hanging fruit" security risks, i.e., those risks that were relatively cost-effective to mitigate in a timely manner.

The "What-If" scenario exploration, augmented by the projected ROI, significantly aided him with this prioritization, providing the financial data needed to allocate resources more efficiently and maximize impact. With the financial implications of various security control upgrades and cybersecurity investments, Schlumpf was able to make more informed decisions and align his strategy with Bystronic's specific risk profile and business goals, ultimately reinforcing the company's cyber resilience.

The quantified insights also strengthened the CISO's communication with senior stakeholders, giving them clear, data-backed metrics to understand the rationale behind his budget requests. With the monetary information, these budget-makers could tangibly understand the necessity of allocating funds to the cybersecurity department.

> *"The ROI calculations make the cyber risk management story more compelling."*