KOVRR
Cyber Decisions. Financially Quantified.

Reducing Incidents by 50% With a Data-Driven Cybersecurity *Strategy*

Investment Management Organization's CISO Helps Prioritize Resources and Reduces Risk With CRQ

www.kovrr.com

Table of Contents

Overview of Company

The company is an Australian-based investment management organization that handles over $100 billion AUD in assets.

The Problem

The Chief Information Security Officer (CISO) at the investment management organization arrived at his current position as a seasoned user of cyber risk quantification (CRQ). In his previous role, the CISO was tasked with managing the risk associated with protecting millions of data records across the globe within multiple decentralized business units. Consequently, he turned to CRQ to assess the economic impact of a cyber scenario affecting both the entire organization and individual business units during a period of major business changes, including M&A activity and divestment.

By implementing CRQ, the CISO was able to communicate to the executive leadership team the most likely cyber scenarios to occur within the short term, which could disrupt the business from achieving its objectives and delay the execution of the major transformational work. The data-driven CRQ forecasts empowered the CISO to take a targeted approach to enterprise risk management by securing a budget for a major cybersecurity uplift program to help mitigate the cyber risks across the business and, in particular, the business units going through considerable structural changes.

When the CISO started at the investment management company last year, his primary goals were **to create an uplift program that focused on resilience, help strengthen the organization's cybersecurity posture, and align cyber risk levels with the board's overall risk appetite statement**. Capitalizing on his previous success with CRQ, one of his first initiatives was to run a quantification assessment to gain an in-depth understanding of the most significant cyber risks specific to the investment management organization.

However, the CISO needed to take the new stakeholders with him on the CRQ journey, which was a new concept for the business. Their buy-in was critical for getting a new strategy approved and subsequently implemented.

Achieving Stakeholder Buy-In

While the investment management organization’s leadership team and board members were relatively advanced in cybersecurity matters, generally understanding CRQ outputs, both the chief risk officer and chief executive of technology were curious about the methodology used to provide a forecasted financial impact within the next 12 months. They requested more transparency regarding the data that was being fed to the CRQ, the exact cost inputs behind the loss scenarios, as well as deeper justifications as to why CISO was recommending to reallocate the budget and reprioritizing various cybersecurity control upgrade projects over others.

Aligning Risk Appetite Levels With Cyber Reality

After being presented with the results of an initial quantification, these key stakeholders originally concluded that the investment management organization’s average financial

exposure due to a business interruption was not materially above the enterprise risk management consequence thresholds and, therefore, wanted to understand the sliding scale of exposure CRQ was articulating.

The CISO, however, with the aim of being efficient with the allocated funding, wanted to minimize the chances of these unbudgeted, otherwise unplanned expenses materializing. He, therefore, needed to provide evidence that bolstered his conviction that implementing additional proactive preventative and detective controls to help reduce the residual risk of a major cybersecurity incident impacting the business and its customers was, in fact, both necessary and a prudent, economical choice.

Assessing Third-Party Risk and Demonstrating Due Diligence

A few months into his new role as the CISO, the investment management organization announced that it would be entering into a major strategic partnership with a third-party service provider. This switch introduced two additional hurdles the CISO would have to address, the first of which was updating the new cybersecurity uplift strategy to incorporate the risk associated with the support model offered by this service provider.

The second issue was that, due to its status as a publicly listed company on the Australian Stock Exchange and an APRA-regulated company, the investment management organization needed to adhere to specific Australian Securities & Investments Commission (ASIC) and APRA Prudential Standards regarding cybersecurity risk management practices. For instance, under CPS 234, APRA-regulated entities must "assess [the] information security capabilities" of any third party that manages information assets on behalf of the regulated entity.

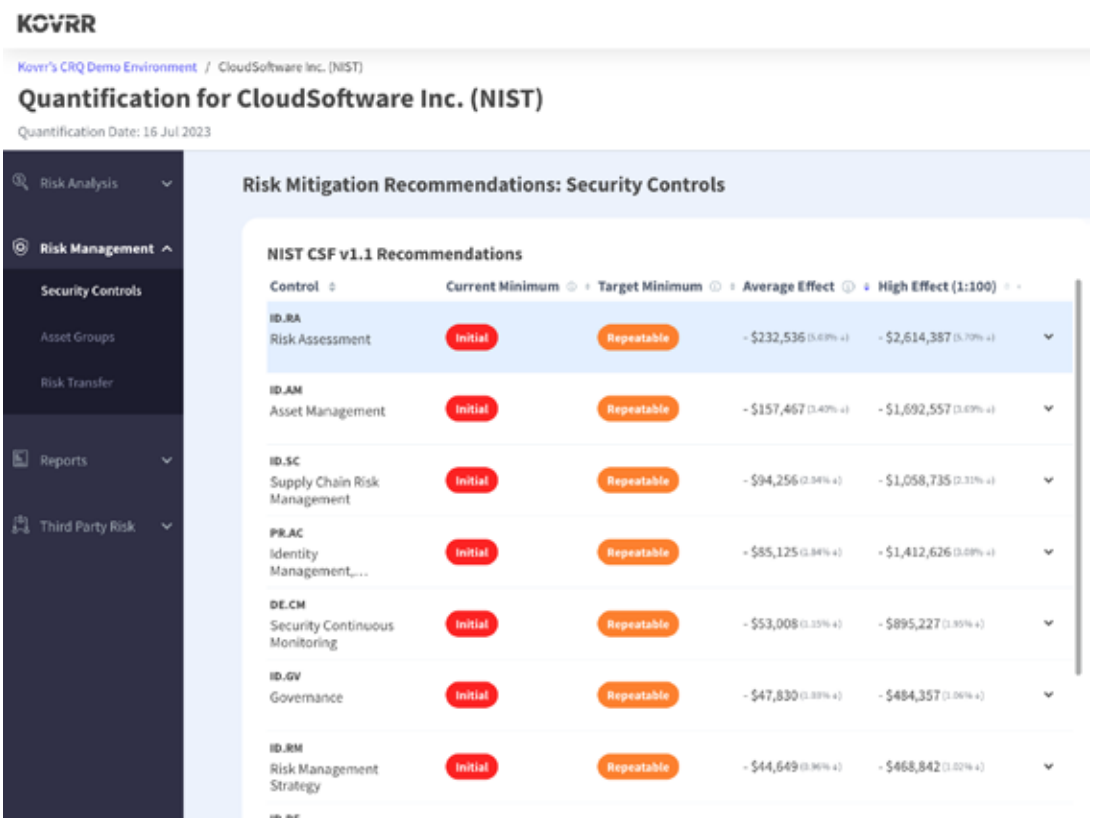
In addition to these existing obligations, the investment management organization is also preparing for the new CPS 230 Operational Risk Management Standard, mandating that APRA-regulated entities effectively manage the risks associated with service providers by establishing comprehensive service provider management policies, formal agreements and robust monitoring processes. Therefore, the CISO was tasked with verifying that his team performed the appropriate due diligence on this new material service provider while avoiding the traditional risk qualification process, which is often deemed subjective and not data-driven

The Solution

To ensure that the CRQ results accurately reflected the investment management organization's current cybersecurity posture, the CISO aligned inputs with the organization's respective implementation tiers for each of the categories within the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), amalgamated other crucial internal data, and ran a subsequent quantification leveraging the Monte Carlo simulation methodology.

The CRQ approach thus incorporated both this internal information and external global intelligence gathered from dozens of continuously updated data sources, ultimately providing the CISO with data-driven forecasts of the loss scenarios the investment management organization was **most likely** going to face in the upcoming year due to cyber activity.

> *"It was seamless and took less than a week. I obtained access to the portal to run the quantification, I received the results almost immediately, and then I incorporated the key data points into the cybersecurity strategy."*



CRQ illuminates the average and high effects of security control upgrades according to specific cybersecurity control frameworks.

Furthermore, because CRQ illuminates the average and high effects of various security control upgrades according to the most common cybersecurity frameworks, including the NIST CSF, the CISO was able to hone in on the specific controls that would most effectively reduce the investment management organization's financial exposure due to cyber risk, leveraging these findings to drive the overall cybersecurity uplift program. He likewise utilized the common business language of NIST (e.g., Govern, Identify, Protect, Detect, Respond, and Recover) to justify resource allocation and budget requests, thereby helping to facilitate collaboration amongst non-technical colleagues and stakeholders.

> *"When you're talking in a business language, going through all the controls that you're seeking investment in, and using data from risk quantification...not many people can discredit the process or justification to fund the initiatives. It just leads to an adult conversation with key stakeholders about risk vs reward due to the robust methodology being used."*

Finally, to support the investment management organization in its third-party cyber risk assessment and demonstration of due diligence, the CISO extended his use of CRQ to evaluate the third-party service provider. The CISO was then able to gain crucial, quantified insights regarding the third-party service provider's risk and the additional operational risks it opened the investment management organization up to as a result of the new partnership.

The Outcome

Conducting a CRQ assessment equipped the CISO to draft a data-driven uplift strategy built upon a framework with which key executives were already familiar. He then used these assessment results to **steer the conversation** and demonstrate that mitigation proposals were based on scientific findings rather than subjective interpretation. This communicable objectivity persuaded the leadership team of the validity of the strategy and, subsequently, **garnered their full support**.

Similarly, CRQ's scalability facilitated a more informed decision-making process in the boardroom. By adding only a few more data points to the quantification inputs, making follow-up results even more tailored to the investment management organization's unique cyber risk posture, the CISO was able to convince the leadership team and board that their financial exposure due to a business interruption was significant enough to warrant additional investment in building resilience and, thus, **the cybersecurity uplift strategy was approved.**

> *"When I presented the strategy to the leadership team, they actually got the concept behind how we can build a resilient organization; CRQ brought the topic into more of a business conversation and made it easier for them to understand why I was looking for investment to uplift the control framework."*

Simultaneously, because the CISO evaluated the cyber risk of the material service provider, the investment management organization **successfully illustrated that it performed its due diligence using credible methodologies**, highlighting that the scenario most likely to cause significant loss was a business interruption, as opposed to data theft or ransomware.

Using CRQ to Drive Cybersecurity Control Maturity

When operating within a highly innovative, inertia-focused organization such as this particular investment management organization, a retroactive approach to cybersecurity would be impractical. That's why the CISO's uplift program was more proactively focused, emphasizing control improvements using the NIST CSF.

By assessing the investment management organization's exposures according to its current control levels, the CISO was able to understand precisely which business areas would be more likely to incur an impact on business operations in the next 12 months

and, consequently, put measures in place to reprioritize both human and financial resources to help mitigate the risks materializing.

Using this information, the CISO garnered the support and resources to build a data-driven strategy that aimed to increase maturity levels by 50% by June 2024 and an additional 17% by the following year. To date, the strategy has also helped reduce incidents by 50% compared to the previous 12 months. Thanks to CRQ, the CISO's team is well-equipped and tracking well with the cybersecurity uplift program.