KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

6 Reasons Why CISOs Need to Embrace Financially Driven Cyber Risk Quantification (CRQ)

MARCH 2022

The job of a chief information security officer (CISO) can be rife with uncertainty and difficulty in terms of getting alignment and buy-in from other stakeholders. As serious as cybersecurity is, the abstract of the way cyber risk is often reported , makes it hard for decision-makers such as board directors and other executives to fully grasp what's at stake. However, CISOs can overcome these challenges through methods like cyber risk quantification (CRQ). Through CRQ, organizations can calculate what their cyber risk means in financial terms. Knowing how much money is at stake in the event of various cyber incidents can help everyone understand cyber risk more concretely, while making it easier to then make decisions around managing this risk. To calculate value at risk, CISOs can leverage automated CRQ platforms that can help CISOs:

01 Assign a financial value to cyber risk

Telling other executives, like your CEO or CFO, that a cyber attack could cause serious financial damage may get their attention, but it's hard to consistently get the response you want when putting cyber risk in these relatively vague terms. Instead, assigning a specific financial value to cyber risk helps motivate corresponding action. Saying that $1 million is at stake, for example, rather than $100,000, could lead CISOs to get approval for a more appropriate security budget.

02 Understand the businesses overall exposure to cyber risk

One of the key challenges is understanding the businesses overall exposure to cyber risk. Having a solid financial reference point that you can measure progress against is critical in enabling decision-makers to assess progress or reflect changes in the risk landscape as they occur. Understanding the overall exposure will also help deliver a clearer delineation into the different cyber risk management choices such as: Mitigation, risk transfer or acceptance.

KOVRR
Cyber Decisions. Financially Quantified.

03 Prioritize cyber security investments and controls

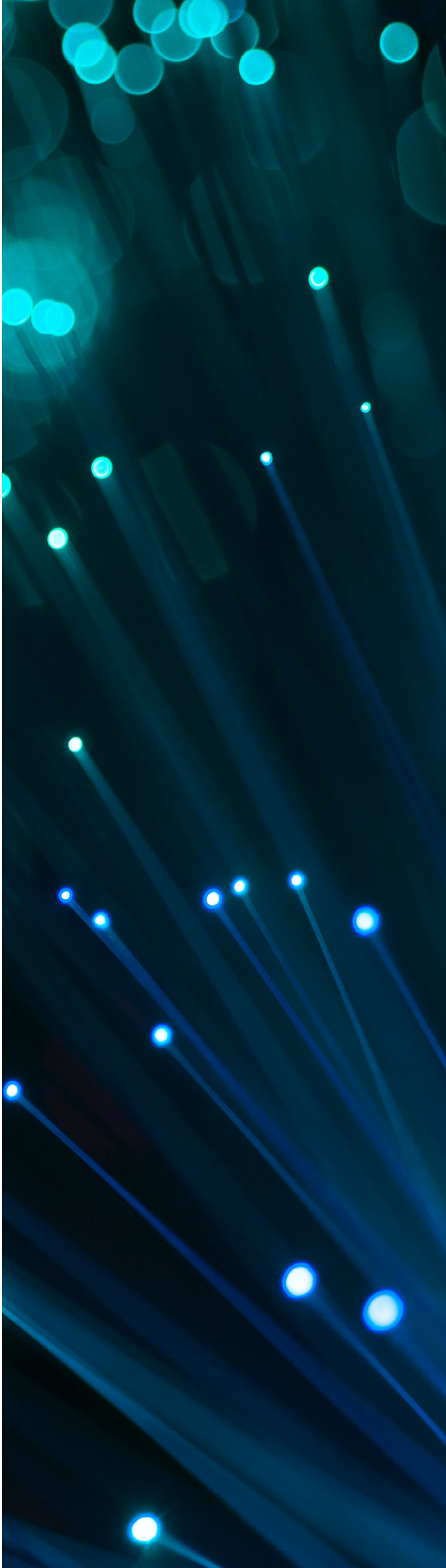
Building off the ability to assess risk transfer decisions, CRQ can help CISOs clarify how to prioritize security measures. Financial quantification and risk management go hand in hand, because even if you can't negate all risk, you can focus your resources toward the areas that have the potential for the most financial damage. For example, a company might realize that prioritizing data recovery capabilities would have the largest effect on reducing financial risk. So, you might focus on that area before turning to lower priority measures, such as implementing a security awareness and training program. But the specifics can vary among different organizations, so that's why it's important to model what CRQ means for your own enterprise.

04 Assess cyber insurance & risk transfer decisions

Once you know the monetary value of cyber risk facing your enterprise, you can decide whether to accept, mitigate, or transfer the risk. For example, if your organization is weighing whether or not to purchase cyber insurance, calculating the financial implications of a cyber attack can help you determine the cost/benefit of transferring this risk to insurance. In other cases, you might decide that a low monetary risk associated with certain cyber events means it isn't worth putting additional resources into improving defenses in that area, at least until you can shore up more pressing areas first.

05 Analyze technology decisions

Related to prioritizing security measures, CRQ also helps with analyzing technology decisions. If you want to shore up your defenses in high-risk areas, CRQ can help you define those risks and analyze what would happen if you invested in various technologies. That way, you can determine what technologies to prioritize and convince other stakeholders to implement new tools. Your CTO, for example, may be more willing to invest in new security tools if there's a clear cost/benefit.



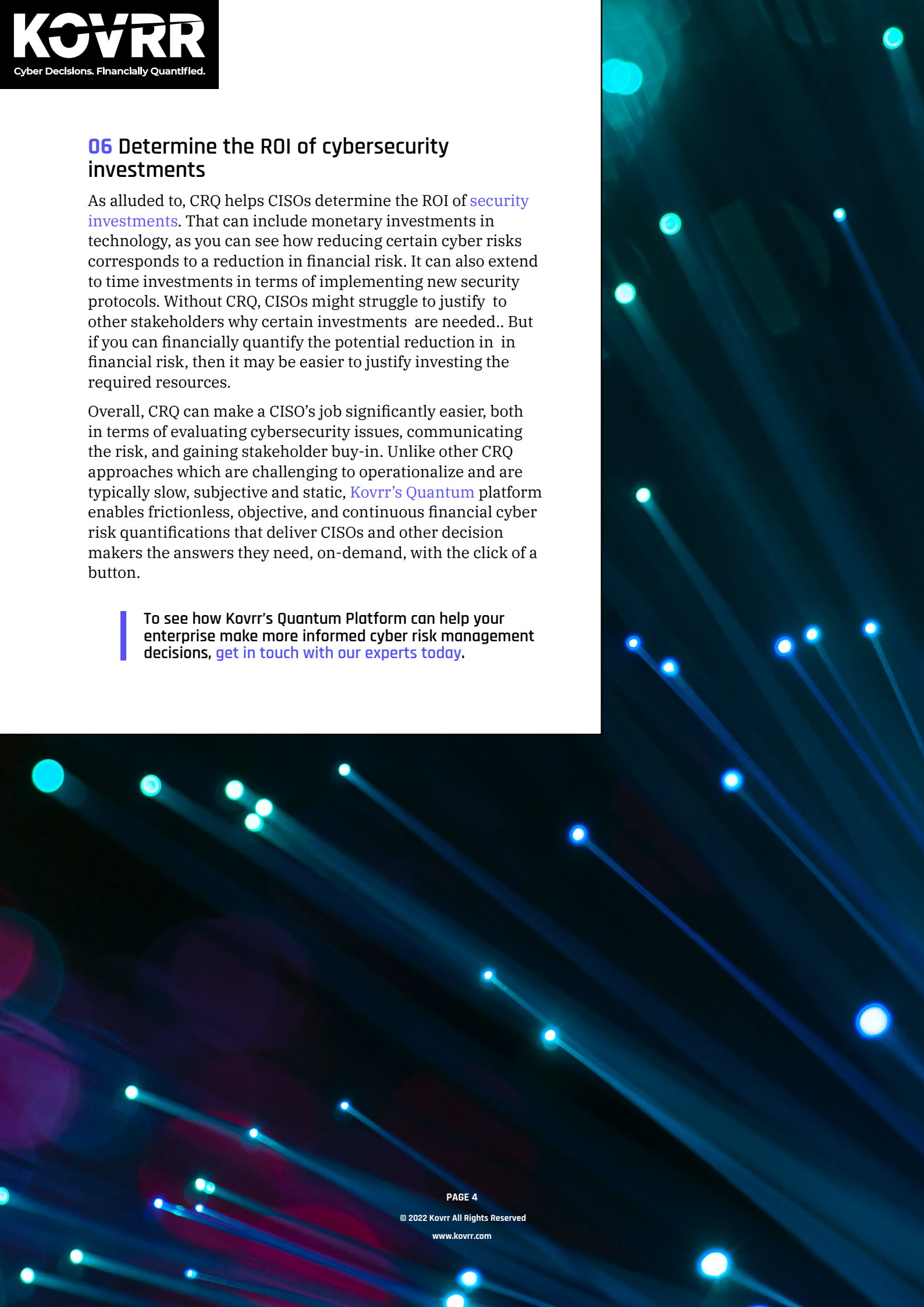
KOVRR
Cyber Decisions. Financially Quantified.

06 Determine the ROI of cybersecurity investments

As alluded to, CRQ helps CISOs determine the ROI of security investments. That can include monetary investments in technology, as you can see how reducing certain cyber risks corresponds to a reduction in financial risk. It can also extend to time investments in terms of implementing new security protocols. Without CRQ, CISOs might struggle to justify to other stakeholders why certain investments are needed.. But if you can financially quantify the potential reduction in in financial risk, then it may be easier to justify investing the required resources.

Overall, CRQ can make a CISO's job significantly easier, both in terms of evaluating cybersecurity issues, communicating the risk, and gaining stakeholder buy-in. Unlike other CRQ approaches which are challenging to operationalize and are typically slow, subjective and static, Kovrr's Quantum platform enables frictionless, objective, and continuous financial cyber risk quantifications that deliver CISOs and other decision makers the answers they need, on-demand, with the click of a button.

> To see how Kovrr's Quantum Platform can help your enterprise make more informed cyber risk management decisions, get in touch with our experts today.



The Author

Gil Hazaz

VP Sales, Enterprise Solution

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: contact@kovrr.com