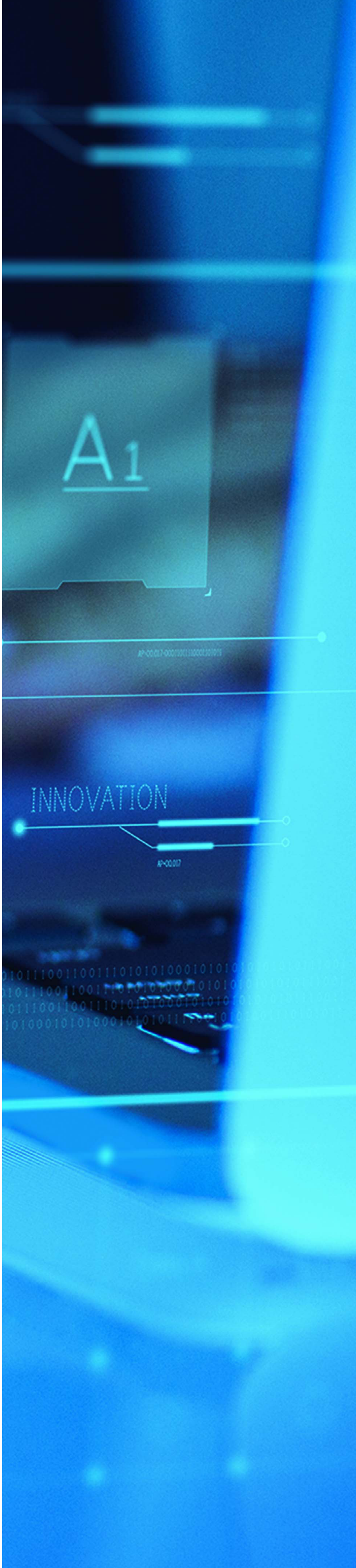
KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Utilizing CRQ to empower a shared cybersecurity accountability approach

FEBRUARY 2022



While many organizations designate a single person as their cybersecurity lead, such as a chief information security officer (CISO), relying on one individual may not be the best approach. Instead, many security experts and researchers believe that the best way forward is to share cybersecurity accountability and responsibility across a leadership team.

That's not to say that a CISO, chief information officer (CIO), IT manager or similar leader can't take a central role when it comes to cybersecurity. Rather, they shouldn't be the only ones at the table.

Other key stakeholders such as CEOs, chief operating officers (COOs), board directors, and lines of business managers should also likely be involved and share at least some accountability/responsibility.

These other leaders can have valuable insights into different areas of the business that affect cybersecurity strategy. And they also may have the capabilities to execute that strategy based on their day-to-day duties that differ from high-level CISO activities.

"As cybersecurity pervades every aspect of an organization, it needs to be embedded in business and decision-making conversations. The phrases 'cyber everywhere' and 'secure by design' become meaningful as they bring trust and security to decisions," notes Deloitte.

In this article, we'll dive more into why a shared model is the way forward and take a look at how to implement this approach.

Cybersecurity Affects Business Issues

A key reason why cybersecurity accountability should be shared is that cybersecurity directly affects business issues. A ransomware attack, for example, isn't just limited to IT figuring out how to remedy the attack and restore data access. It can also affect areas like PR, considering that companies could need to manage public perception of the attack, especially if sensitive customer information leaks.

In fact, 88% of boards of directors (BoDs) think of cybersecurity as a business risk, rather than just a technology risk, finds Gartner.

"Gartner recommends that IT and security leaders work with executives and BoDs to establish governance that shares responsibility for business decisions that affect enterprise security," the research firm notes.

The good news is that more companies are starting to realize that cybersecurity is an enterprise-wide issue.

For example, a 2021 KPMG global survey finds that CEOs ranked cybersecurity as the top risk to their organization's growth over the following three years. In comparison, cybersecurity ranked fifth in the previous year's survey.

Implementing Shared Accountability

By taking a more collective approach, businesses can get a more thorough understanding of the risks they face and figure out ways to strengthen their defenses.

A CISO might have clarity on emerging cyber threats, for example, but they might not have the same day-to-day oversight over sales teams to make sure they're following corresponding protocols when handling customer data. Instead, that responsibility could fall into sales managers, or perhaps an executive like a COO, depending on the company's structure.

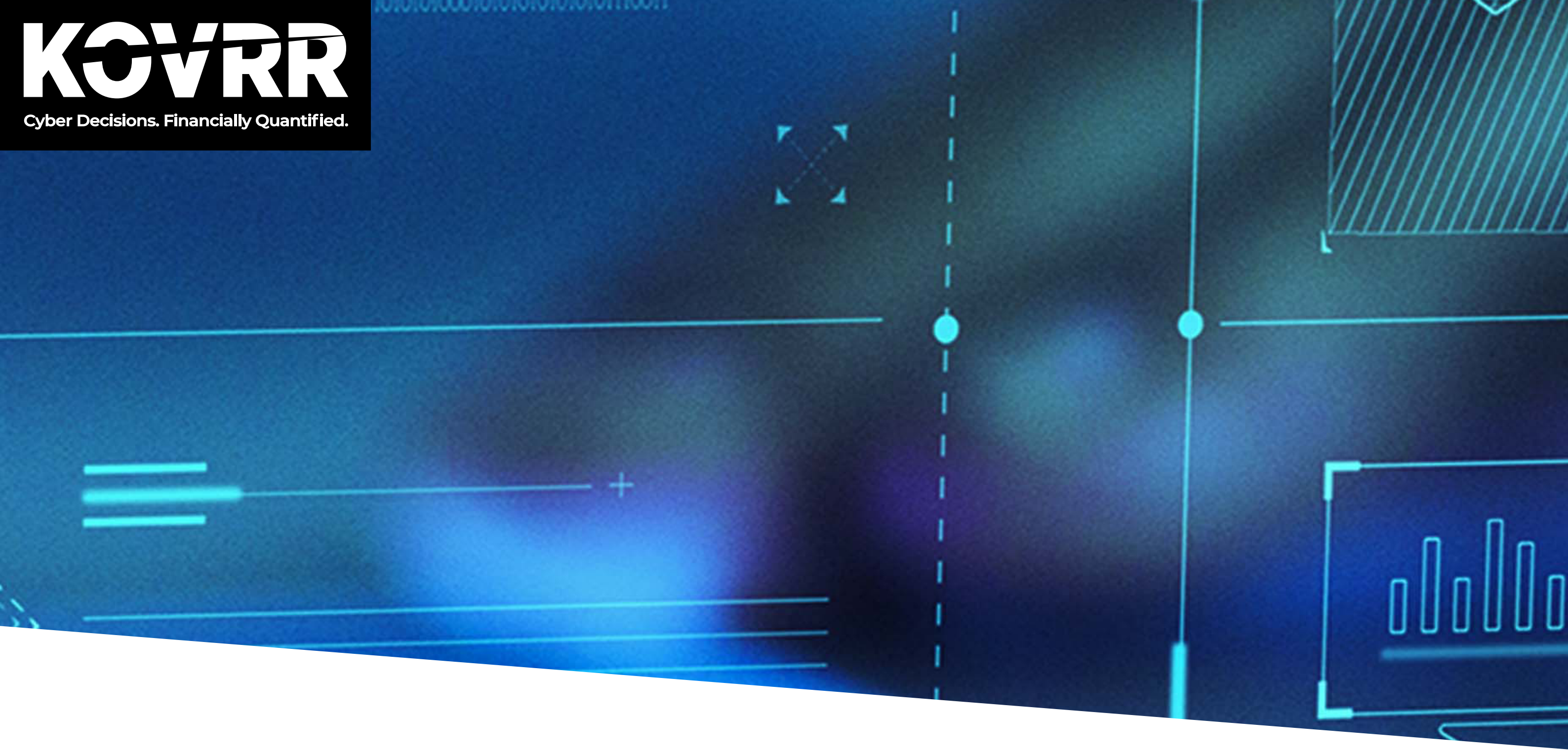
Getting to that point, however, could require current leaders, such as CISOs, to put more effort into helping other executives and lines of business managers fully understand what's at stake.

"CISOs should articulate to the board and executives how cyber security plays into all decisions...Integrating into corporate strategy involves a more holistic approach to business, moving out of the technological comfort zone and becoming storytellers," advises KPMG.

One way to tell clear stories and put cyber risk in business terms is to use solutions such as Kovrr's Quantum cyber risk quantification platform.

Doing so can quantify cyber risk in financial terms, which can help non-technical leaders understand exactly what's at stake. From there, executives and other key stakeholders can prioritize cybersecurity defenses based on financial risk and potential reduction of it. That can be a natural way to keep other leaders, such as CEOs and CFOs, engaged and accountable when it comes to cybersecurity.

> **Want to see how Kovrr Quantum's financial modeling can help you implement a shared accountability approach? Book a demo with our experts.**



The Author

Tom Boltman

VP Strategic Initiatives

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