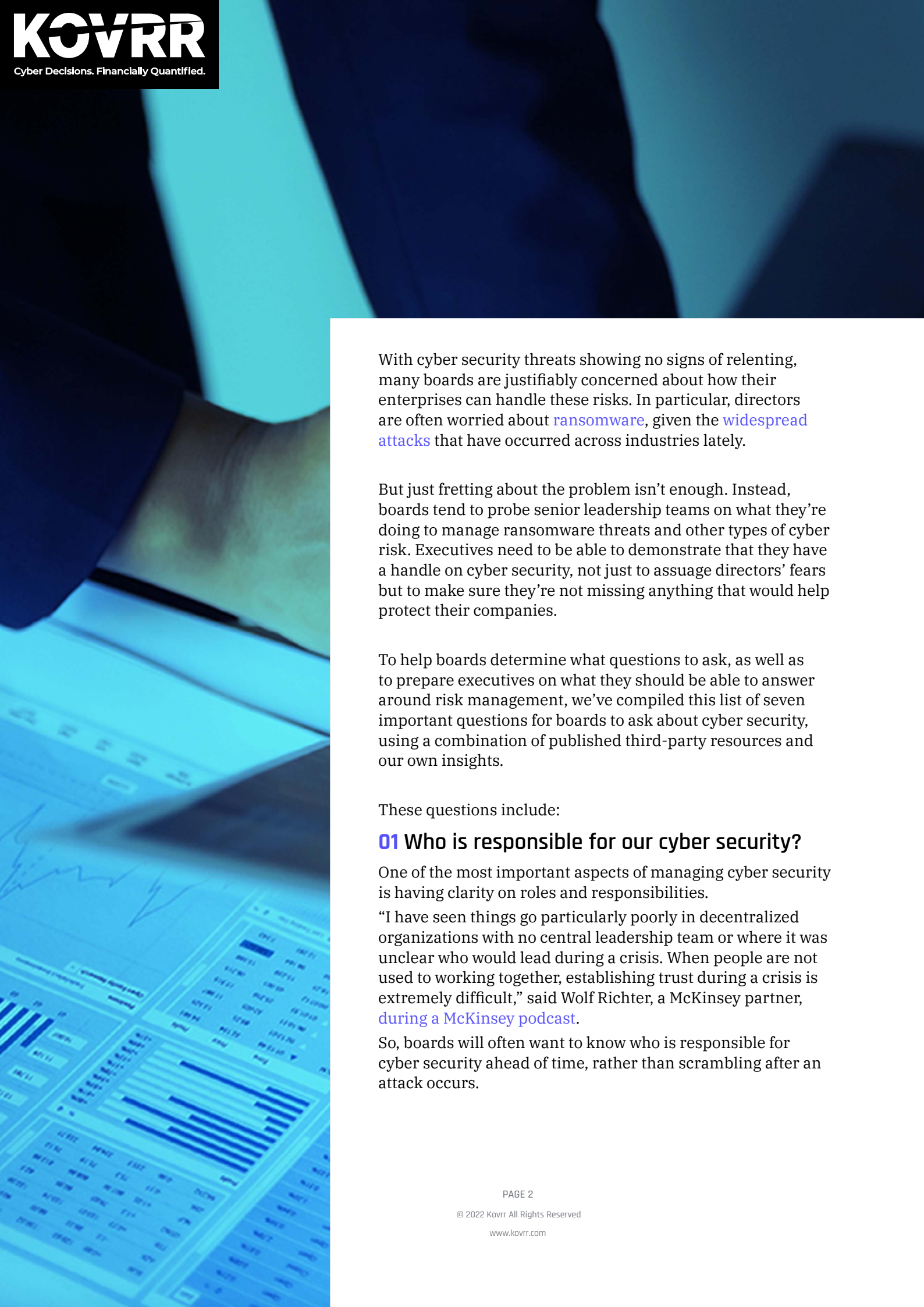
KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

7 Questions Boards Must Ask About Cyber Risk

MARCH 2022



With cyber security threats showing no signs of relenting, many boards are justifiably concerned about how their enterprises can handle these risks. In particular, directors are often worried about ransomware, given the widespread attacks that have occurred across industries lately.

But just fretting about the problem isn't enough. Instead, boards tend to probe senior leadership teams on what they're doing to manage ransomware threats and other types of cyber risk. Executives need to be able to demonstrate that they have a handle on cyber security, not just to assuage directors' fears but to make sure they're not missing anything that would help protect their companies.

To help boards determine what questions to ask, as well as to prepare executives on what they should be able to answer around risk management, we've compiled this list of seven important questions for boards to ask about cyber security, using a combination of published third-party resources and our own insights.

These questions include:

01 Who is responsible for our cyber security?

One of the most important aspects of managing cyber security is having clarity on roles and responsibilities.

"I have seen things go particularly poorly in decentralized organizations with no central leadership team or where it was unclear who would lead during a crisis. When people are not used to working together, establishing trust during a crisis is extremely difficult," said Wolf Richter, a McKinsey partner, during a McKinsey podcast.

So, boards will often want to know who is responsible for cyber security ahead of time, rather than scrambling after an attack occurs.

02 What does our incident response plan look like?

Related to knowing who is responsible for different aspects of the company's cyber security ahead of time, boards often also want to know more details about what an actual incident response plan would look like.

"Organisations should think in terms of 'when' rather than 'if' they experience...a significant cyber incident. So it's essential to plan your response carefully and to practice (or 'exercise') your response," notes the UK's National Cyber Security Center.

03 What's financially at stake?

Another important area for boards to understand is what cyber risk means in financial terms. If senior leadership can demonstrate what cyber incidents could equate to in terms of monetary costs, then boards may be able to better conceptualize what the company should do next. Enterprises can use cyber risk quantification (CRQ) models to explain cyber risk in financial terms.

In some cases, when financial quantification shows relatively low amounts of potential financial damages are at stake, boards and executives may be more comfortable accepting the current risk. Yet when the financial stakes are higher, they might prefer to take mitigating action like adding cyber security technology. Or, they might decide to transfer more financial risk via cyber insurance.

04 What are our cyber security investment priorities?

Understanding cyber risk in terms of financial quantification can then make it easier for boards to ask about cyber security investment priorities. Depending on what's at stake and where the largest vulnerabilities exist, companies might make varying levels of investment in risk management areas like hiring IT staff, implementing employee security training programs, and adding cyber security software tools.

Ideally, companies can use CRQ to justify investment priorities, such as by modeling how investing in security awareness and training programs would reduce financial risk.

05 What do other cyber events and emerging trends mean for our company?

Boards also want to know what companies are doing to reduce the risk related to emerging trends, some of which may hit close to home. If they see that a competitor has been affected by a new ransomware variant, for example, they likely want to know what that means for their own organization.

"Board members encounter threat reports, articles, blogs and regulatory pressure to understand risks. They will always ask about what others are doing, especially peer organizations. They want to know what the 'weather' looks like and how they compare to others," explains Gartner.

While executives can't always predict what's going to happen, they can demonstrate what they are doing to stay informed and how they can adapt the company's defenses as new threats become clearer.

06 How do we manage the cyber risk related to vendors/partners?

In addition to staying on top of internal threats, boards also often want to know what their companies are doing to manage the cyber risks that third parties like vendors can introduce.

Although companies might have limited control over what their vendors and partners do, they can still evaluate the cyber preparedness of third parties and see whether it makes sense to continue working with them.

"With cyberthreats becoming more sophisticated and pervasive, it greatly benefits businesses to have proactive security mechanisms across the entire organizational ecosystem, including with business partners, contractors and other vendors – ensuring these third-parties have acceptable levels of cybersecurity," notes Deloitte.

07 How does remote work affect our cyber security plan?

Lastly, depending on where an organization is in terms of hybrid or remote working arrangements, boards may be asking more recently about what that means for cyber security.

Executives can explain to boards the details of how they're accounting for new cyber risks related to remote work, such as by adjusting authentication practices and device management.

"If your company took short-cuts to expand remote connectivity, you should prioritize doing an assessment that reviews access, the current controls in place (established for a different world) and the threats your remote workers may inadvertently be creating," notes PwC.

Overall, boards are often taking a closer look at cyber security, and executives should be prepared to answer questions around both internal and external approaches. Using CRQ tools, such as Kovrr's Quantum platform, can help companies understand what's at stake financially, which can then make it easier to prioritize security measures, analyze technology investments and more.

Quantum's data-driven approach is built from the ground up to enable evolving, objective, and frictionless financial cyber risk quantifications that deliver the board, CISO, CRO and other decision makers the answers they need, on-demand, with the click of a button.

> **To see how Kovrr's cyber risk quantification models can help your enterprise strengthen cyber security, get in touch with our experts today.**

The Author

Yakir Golan

CEO

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