KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Midmarket Companies Getting Caught in Ransomware Crosshairs: Are PE Firms Ready?

MAY 2022

When you think of cybercrime affecting the finance industry, your thoughts might go to the banking sector or multinational financial conglomerates. Yet these are far from the only areas of finance at risk for cyber-attacks. Private equity firms also face significant cybersecurity threats.

Even though more progress has been made in recent years to address PE cyber risk, many firms fail to fully quantify how cyber events could impact their portfolios. And in many respects, the risks are only increasing.

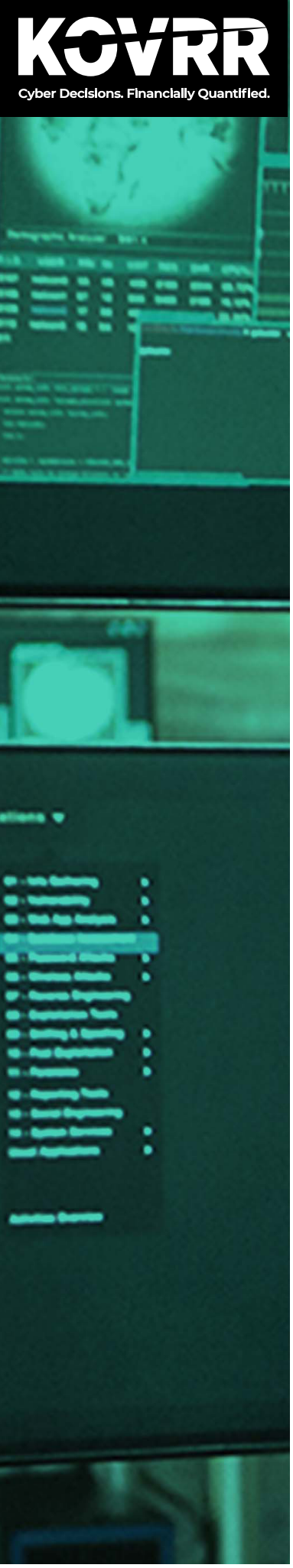
As a Wall Street Journal article notes, "ransomware groups are turning their attention to midmarket acquisition targets, presenting a risk for private equity, venture capital and other deal makers that often invest in such businesses."

To that point, a February 2022 joint advisory from cybersecurity authorities in the U.S, Australia, and U.K. says that ransomware attackers are shifting focus from large targets to "mid-sized victims to reduce scrutiny."

So, on one hand, PE firms could face cybersecurity risks regarding their internal operations, such as with all the assets and financial data they hold involving limited partners (LPs). You don't have to be a prominent investment firm to still be a target. At the same time, due to PE firms' reliance on third-party vendors, such as fund administrators, PE firms are also at risk if their providers are attacked.

On the other hand, PE firms also face cyber risks regarding their portfolio companies, with attacks potentially affecting valuations. As Deloitte notes, "while cyber incidents may begin as a technology issue, they typically extend well beyond the technology domain and hit at the very heart of business value and performance." Even if a breach is contained to one portfolio company, that could derail that investment, such as if the attack causes the company to bear the cost of remediation and lose customer trust.

Yet, as we'll explore in this article, there are ways that PE firms can improve how they account for these risks. With cyber risk quantification — which involves measuring the financial value at risk due to cyber events — PE firms and other asset managers can better understand their exposure both internally and amongst portfolio companies. Doing so can help attract LP investment, and increase the likelihood of success for portfolio companies.



Meeting New LP Demands

Part of why it's so important to improve financial quantification and risk management is to meet new LP demands around cybersecurity.

For example, in November 2021, the Institutional Limited Partners Association (ILPA) — whose members include some of the world's largest institutional investors — updated its due diligence questionnaire to include questions about areas like data security. This questionnaire asks general partners (GPs) for both open-ended and yes/no responses that can help LPs more precisely evaluate the cybersecurity protocols that a PE firm has in place.

Some of the questions are more tactical, like whether sensitive data is encrypted (both when stored and in transit) and whether firms carry out activities like penetration testing. Others are somewhat broader, asking about areas like how PE firms work "with portfolio companies (where the Firm holds a significant or controlling interest) to implement a cyber/information security policy and the types of standards, testing, and third-party assessments in use by portfolio companies."

So, PE firms will likely face these types of questions more from LPs. Even if an investor is not part of the ILPA, this updated questionnaire points toward a shift among LPs to understand how PE firms are specifically approaching cybersecurity inside the asset management firms and their portfolio companies. Having clear security plans and protocols in place could then help GPs meet LPs' due diligence requirements.

Continuously Quantifying New Risks

In addition to meeting LPs' demands, PE firms can potentially reduce operational risk and make more informed investment underwriting decisions through cyber risk quantification (CRQ).

Software solutions such as Kovrr's Quantum platform enable organizations to see what their particular level of cyber risk translates to in financial terms.

Not all cyber events will have the same financial impact, and some events may be more costly for certain types of companies, depending on factors like the technology and data they have in place. Also, taking different types of cyber risk management actions can drive different results in delivering financial value.

KOVRR
Cyber Decisions. Financially Quantified.

So, PE firms can use these CRQ tools to make more informed cybersecurity decisions. For example, quantifying the financial impact of areas like improving cybersecurity training vs. adding new security controls can help PE firms prioritize their cyber risk management decisions. They can also more clearly analyze the ROI of operational cyber investments.

CRQ can also help when it comes to evaluating investment opportunities at a portfolio company level. If deciding between two companies to acquire, for example, knowing that one company has a higher financial risk due to cybersecurity gaps could sway that decision and inform pricing.

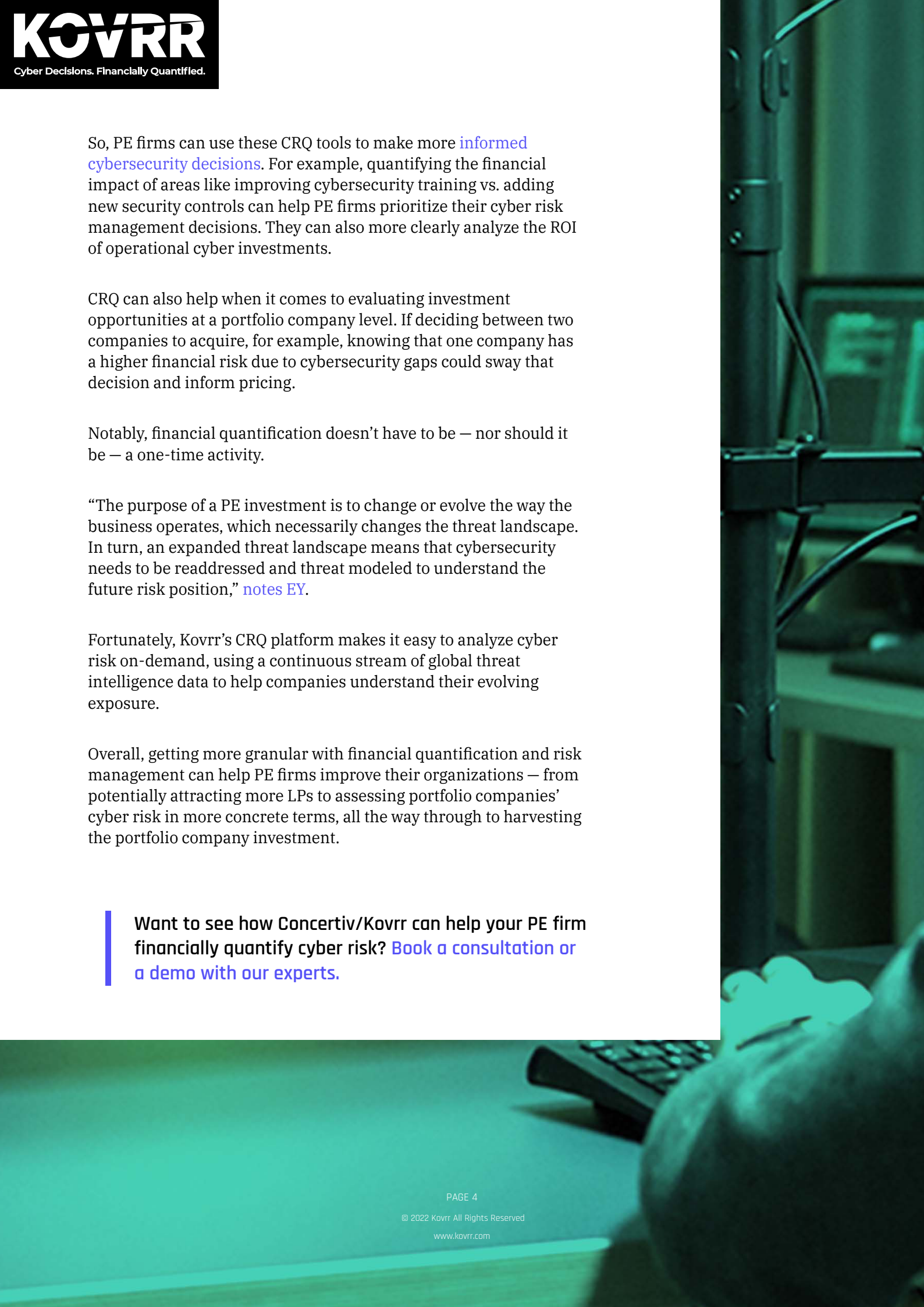
Notably, financial quantification doesn't have to be — nor should it be — a one-time activity.

"The purpose of a PE investment is to change or evolve the way the business operates, which necessarily changes the threat landscape. In turn, an expanded threat landscape means that cybersecurity needs to be readdressed and threat modeled to understand the future risk position," notes EY.

Fortunately, Kovrr's CRQ platform makes it easy to analyze cyber risk on-demand, using a continuous stream of global threat intelligence data to help companies understand their evolving exposure.

Overall, getting more granular with financial quantification and risk management can help PE firms improve their organizations — from potentially attracting more LPs to assessing portfolio companies' cyber risk in more concrete terms, all the way through to harvesting the portfolio company investment.

> **Want to see how Concertiv/Kovrr can help your PE firm financially quantify cyber risk? Book a consultation or 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