KOVRR

Cyber Decisions. Financially Quantified.

The Guide for Moving From Qualitative to Quantitative Risk Assessments

Understanding Cyber Risk Quantification:
From Uncertainty to Insight

www.kovrr.com

Table of Contents

Transitioning from Qualitative Guesswork to Quantified Confidence

Once relegated to the technical corners of the organization, cybersecurity is no longer an isolated problem that can be attended to reactively. Amid the rising costs of cyber incidents and growing regulatory scrutiny, it has become a high-level business risk that requires proactive analysis and mitigation.

Much in the way that business leaders rely on forecasts to manage financial volatility or weather-related disruptions, today's stakeholders likewise need an understanding of their company's cyber exposure long before incidents transpire, empowering them to allocate resources more effectively and build resilience.

Historically, non-technical organizational leaders have depended on qualitative risk assessments to visualize such exposure levels. This approach, which includes color-coded matrices and ordinal scales ranging from "low" to "critical," offers simplicity to an otherwise complex topic. Unfortunately, it also lacks rigor, often obscuring the true magnitude and uncertainty of cyber threats and presenting red flags instead of real numbers.

Today's stakeholders, operating in a market where the quality of one's cyber risk management program has a direct influence over long-term success, require more clarity. They need to understand not only that risk exists but also what it could concretely cost, how likely it is to materialize, and which actions will reduce exposure most cost-effectively.

Making Cyber Risk Measurable and Actionable

That necessity is what on-demand cyber risk quantification (CRQ) solutions were designed to fulfill. Translating vague and subjective assessments into measurable financial and operational terms, CRQ builds the foundation for a robust, business-aligned understanding of the organization's cyber risk exposure, supporting informed decisions across departments.

> CRQ compels executives to confront the inherent uncertainty of cyber risk that qualitative methods tend to conceal. While a quantitative risk model that illustrates a range of possible losses might initially cause concern, it actually brings a new level of transparency that makes the conversation more honest and far more useful.

Once reframed into these tangible terms, cyber risk can more easily be weighed along with other business priorities. Rather than being treated as a siloed concern, cyber risk management becomes a part of the strategic framework, shaping organizational priorities and ensuring the business achieves high-end resilience amidst the costly cyber landscape.

Crucially, CRQ is not a one-off assessment but an evolving capability. The success of a CRQ assessment hinges less on the accuracy of any single model or quantification run but more so on the repeatability, transparency, and utility of the process over time. Reliable CRQ models enable cybersecurity teams to replace intuition with evidence and build lasting confidence in loss estimates, mitigation decisions, and the organization's overall ability to manage cyber risk as a strategic concern.

Qualitative methods had their place in the early days of cyber risk management. They helped many organizational leaders build a safer environment for their companies, but they were never designed to meet the demands of today's landscape. Cyber risk quantification isn't only more accurate; it's more practical. In a world of increasing complexity and accountability, practicality is the ultimate value.

Building a Foundation for Executive Alignment

As with most processes, cyber risk quantification modeling requires initial groundwork to be laid before commencement. Because CRQ outcomes directly impact high-level business decisions such as budgeting, capital allocation, insurance, and risk acceptance, it first demands executive buy-in. Without the C-suite and board's engagement, even the most robust CRQ assessment can easily stall.

Building this cultural readiness requires cybersecurity leaders to manage expectations regarding what cyber risk quantification can accomplish, stressing that CRQ models do not offer mathematical perfection but, instead, provide the objective data necessary to support better decision-making. All key stakeholders, including those from financial, audit, and legal teams, need to be briefed on this reality early on, ensuring CRQ is seen as a tool rather than a catch-all solution.

Moving beyond the traditional risk matrix requires a shift in the way that cyber risk is communicated and operationalized across the business. The transition is not merely about replacing qualitative ratings with numbers. It's about embedding a more rigorous, transparent lens into the company's decision-making fabric. When stakeholders understand the value and limitations of CRQ at the outset, they're more likely to trust the process and leverage the insights it yields.

What is Cyber Risk Quantification (CRQ)?

A CRQ assessment involves measuring an organization's exposure to cyber threats in terms of likelihood and loss scenario impacts, such as financial damage, operational downtime, and the number of compromised data records. Instead of expressing cyber risk as a comparative score or color-coded, subjective descriptor in a matrix, CRQ articulates risk in tangible terms, such as a 29% chance of experiencing a ransomware attack within the upcoming year that will cost the organization $40 million.

It’s the same difference that exists between a vague “partly cloudy with a chance of heavy rain” forecast and an hour-by-hour report that shows exactly when the storm will strike, how intense it will be, and which areas are most likely to be affected.

> That additional level of clarity is what helped the CISO at Bystronic, a global manufacturing company, jump-start his cybersecurity strategy within days of running his first risk quantification. After leveraging Kovrr's CRQ to quickly generate concrete financial insights, the CISO became more equipped to not only prioritize his initiatives but also communicate the business impact of cyber threats to senior leadership.

Indeed, the transition from qualitative evaluation to quantitative risk modeling bolsters an understanding of cyber posture across the business, allowing for more informed, data-driven decisions to be made. Executives and board members, regardless of their technical expertise, can evaluate the ROI of initiatives, justify investments for certain projects or solutions, and align the cyber risk management strategy with the organization's overall risk appetite levels. CRQ provides a common language that helps all parties understand what's at stake and the value of protecting it.

To learn more about what cyber risk quantification encompasses and how to conduct a CRQ assessment, read What Is Cyber Risk Quantification (CRQ)?

Quantifying Risk with Kovrr's On-Demand CRQ Platform

The early days of cyber risk quantification typically saw organizations doing extensive manual work to gather the necessary data, investing heavily in calculation processes, and even hiring costly external service providers who would do everything for them. Eliminating this overhead while retaining the analytical depth, Kovrr developed its on-demand CRQ solution, which automatically leverages real-world threat intelligence and incorporates organizational-specific data to rapidly generate cyber risk insights.

Kovrr's platform provides chief information security officers (CISOs) and other security and risk managers (SRMs) with constantly updated information regarding their business's current cyber exposure. Moreover, this on-demand tool is designed to fit seamlessly into enterprise workflows, integrating with other cybersecurity solutions to ensure consistent visibility into cyber risks.

> For one private equity firm overseeing more than 50 portfolio companies, Kovrr's more advanced CRQ process enabled them to quantify each entity's precise cyber risk posture, compare those exposure levels across the entire portfolio, and, consequently, harness that intelligence to renegotiate their cyber insurance policies, reducing premiums by 17%.

With the ability to model threat scenarios tailored to an organization's sector, geography, and unique digital footprint, Kovrr's CRQ platform delivers the objective, timely, and business-relevant insights needed to manage cyber risk with confidence.

Getting Started: Explore Results in Hours. Gain Deeper Insights Over Time.

Kovrr's onboarding process is designed for speed and simplicity, providing organizations with quantified insights in a matter of hours. In fact, it takes most teams less than a day to complete the initial steps, quickly gaining access to their first iteration of quantified insights. In less than a month, cybersecurity leaders can easily move from these early-stage outputs to a fully developed cyber risk strategy that is communicable at the highest business levels.

In the beginning, most organizations will start by modeling a few high-priority loss scenarios, such as those that are well-understood by non-technical stakeholders or seen as business-critical, such as a ransomware event. This early view doesn't aim to illuminate every risk the company faces; it's designed to offer high-level insights early on in the process that can start informing mitigation strategies.

After the initial quantification runs have been completed, programs can easily evolve, growing in both granularity and precision as more scenarios, controls, and contextual data are incorporated into the CRQ model. This phased, iterative approach ensures CISOs and SRMs gain value from the outset while also leaving room to deepen analysis and refine strategies over time as the company's risk posture and priorities evolve.

Average Timeline of Onboarding and Implementation

DAY 1

Uncover the Business Impact of Cyber Risk

- Learn more about the onboarding process during an orientation session with a dedicated account manager.
- Enrich your cyber data with company modeling and Cyber-Sphere creation to ensure data-driven, tailored results.
- Run your first on-demand cyber risk quantification assessment and start viewing the potential loss scenarios your organization faces.
- Explore granular metrics that identify your top exposure drivers, begin altering inputs, and run the next quantification iterations.

DAY 14

Prioritize Initiatives That Drive Results

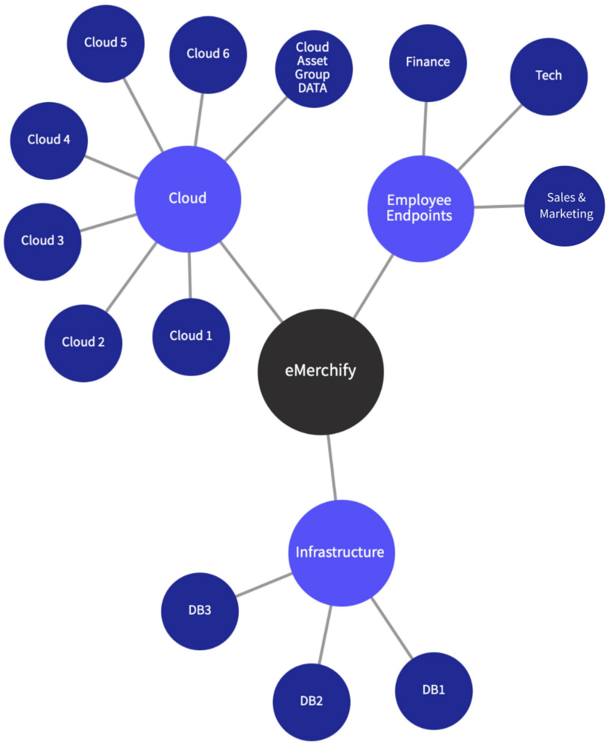
- Leverage data-backed security control recommendations and discover the initiatives that will minimize financial exposure to the greatest extent.
- Evaluate ROI on security investments, gaining the evidence necessary to justify budget spend and request additional resources.
- Analyze third-party cyber risk exposure to inform internal planning. Develop strategies to mitigate risk to a level that aligns with cyber risk appetite.

DAY 28

Communicate Cyber Risk at the Executive Level

- Harness boardroom-ready reports from Kovrr to ensure board members and executives understand the organization’s exposure.
- Equip the leadership team with concrete insights that allow them to establish better cyber governance practices.
- Work with key stakeholders like the CFO to optimize cyber insurance policies and negotiate better terms with data-driven loss forecasts.

Breaking Down the CRQ Onboarding Process



Kovrr's Cyber-Sphere methodology captures an organization's data systems and infrastructure.

Kovrr's cyber risk quantification assessment process is relatively straightforward, providing a structured framework for CISOs and SRMs to illuminate the cyber incidents their organization potentially faces, along with their real-world impact. It begins with the ***creation of the Cyber-Sphere***, Kovrr's proprietary methodology that allows companies to capture the complexities of their infrastructure, systems and networks, and digital footprint at large.

Next, Kovrr ***generates a bespoke event catalog***, leveraging the information modeled in the Cyber-Sphere combined with key characteristic details such as the business's specific industry, region, and technological environment to build an extensive, customized set of cyber risk scenarios the company is likely to face. These scenarios are derived from continuously updated threat patterns and event data sourced from a wide range of real-world intelligence feeds.

The third and final step is to ***run Monte Carlo simulations***, which are essentially "what-if" scenarios that explore how different cyber events could unfold over the coming year. For example, the simulation may find, based on the data, that in one "what-if" year, an organization faces a loss of $4 million due to a single ransomware event, while in another scenario, they face only $1 million in damages because of a business interruption.

In Kovrr's Monte Carlo simulations, we model 25,000 possible versions of this upcoming year, each showing a different way in which cyber incidents may impact a company both financially and operationally. These simulations surface a distribution of potential outcomes, ranging from low-impact disruptions to rare, high-cost tail risks, illustrating how exposure may fluctuate based on severity, likelihood, and context.

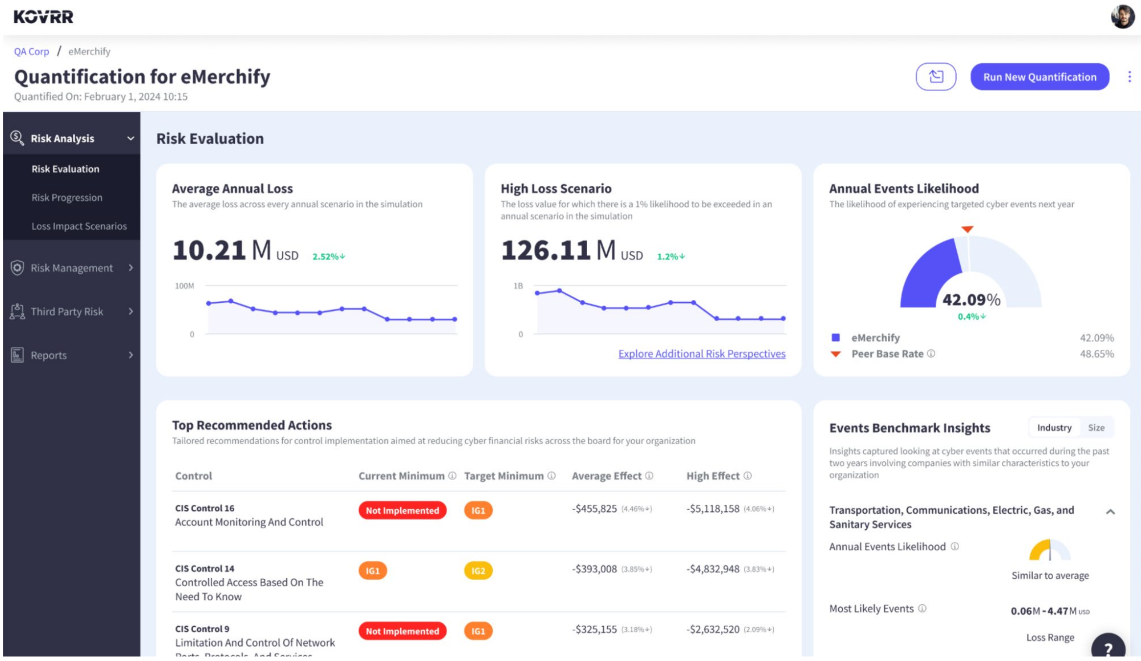
Diving Deeper Into the Modeling Mechanics

Integral to this modeling process is the use of calibrated estimation sessions. During this phase, Kovrr supports cybersecurity teams in working with subject matter experts in the organization to develop a grounded estimate for the evaluated risk scenario. These sessions rely not necessarily on exhaustive data sets, but on defensible assumptions based on organizational knowledge and industry benchmarks.

Introducing concepts like “best-case,” “most likely,” and “worst-case” helps stakeholders build comfort with uncertainty while preserving analytical rigor. By embedding both internal knowledge and external intelligence into the simulations, Kovrr’s modeling approach ensures that CRQ results reflect business realities and provide a transparent basis for decision-making. This enables leaders to confidently assess exposure and articulate the value of mitigation investments.

CRQ Outputs That Power Cyber Risk Decisions

Following the customized simulations, Kovrr's on-demand CRQ solution produces a comprehensive set of outputs that help CISOs and SRMs make crucial decisions regarding their cybersecurity strategies. The data points span technical, operational, and financial dimensions, highlighting loss probabilities, potential business impacts, event durations, attack vectors, and more. Altogether, these insights offer a clear view of an organization's risk landscape and the actions needed to reduce exposure.



Quantification for eMerchify

Quantified On: February 1, 2024 10:15

Risk Evaluation

Average Annual Loss

The average loss across every annual scenario in the simulation

10.21 M USD 2.52%↓

High Loss Scenario

The loss value for which there is a 1% likelihood to be exceeded in an annual scenario in the simulation

126.11 M USD 1.2%↓

Annual Events Likelihood

The likelihood of experiencing targeted cyber events next year

42.09%

0.4%↓

■ eMerchify	42.09%
▼ Peer Base Rate ⓘ	48.65%

Top Recommended Actions

Tailored recommendations for control implementation aimed at reducing cyber financial risks across the board for your organization

Control	Current Minimum ⓘ	Target Minimum ⓘ	Average Effect ⓘ	High Effect ⓘ
CIS Control 16 Account Monitoring And Control	Not Implemented	IG1	-$455,825 (4.46%↓)	-$5,118,158 (4.06%↓)
CIS Control 14 Controlled Access Based On The Need To Know	IG1	IG2	-$393,008 (3.85%↓)	-$4,832,948 (3.83%↓)
CIS Control 9 Limitation And Control Of Network Ports, Protocols, And Services	Not Implemented	IG1	-$325,155 (3.18%↓)	-$2,632,520 (2.09%↓)

Events Benchmark Insights

Insights captured looking at cyber events that occurred during the past two years involving companies with similar characteristics to your organization

Transportation, Communications, Electric, Gas, and Sanitary Services

Annual Events Likelihood ⓘ — Similar to average

Most Likely Events ⓘ — 0.06M - 4.47M USD Loss Range

Kovrr’s CRQ Risk Evaluation dashboard highlights crucial cyber risk metrics for decision-making.

Key Outputs Include:

- **Average Annual Loss (AAL):** The average financial loss from cyber events across simulations for the upcoming year.
- **1:100 Annual Loss:** A high-severity loss value that has a 1% likelihood of being exceeded in the upcoming year.
- **Annual Events Likelihood:** The likelihood of experiencing a cyber event or events that result in loss during the upcoming year.
- **Loss from an Event:** The median value of financial loss the organization is expected to incur should it experience an event.
- **Event Duration:** The median value of downtime (hours) the business is expected to face in the event of an outage.
- **Data Records Compromised:** The median number of data records that will be compromised if the organization is breached or infiltrated.
- **Event Benchmarks:** Comparative insights highlighting the likelihood of experiencing cyber events that result in loss across industries and revenue bands.
- **Risk Drivers, Event Types, Initial Attack Vectors:** A breakdown of the types of events and attack vectors that contribute most to the expected financial loss assessments.

  > The information security officer (ISO) at Moodle, for instance, used these targeted control recommendations to support funding decisions and articulate a data-backed risk reduction plan to the board

- **Top Recommended Actions:** Tailored suggestions for cybersecurity framework control upgrades, detailing which ones will reduce financial losses to the greatest extent.
- **Loss Impact Scenarios:** Financial outcomes tied to specific cyber threat scenarios, such as business interruption, ransomware and extortion, or regulations and compliance.
- **Annual Exposure Loss Distribution Curve:** The full range of potential loss amounts an organization may face in the upcoming year and their respective likelihoods.
- **Business Impact Scenario Loss Distribution Curve:** A detailed look at the likelihood of various loss impact scenarios occurring according to their forecasted loss amounts.

With massive amounts of critical data generated from the Monte Carlo simulations, translated into actionable outputs, decision-makers can move from analysis to execution, driving the business further towards its goals.

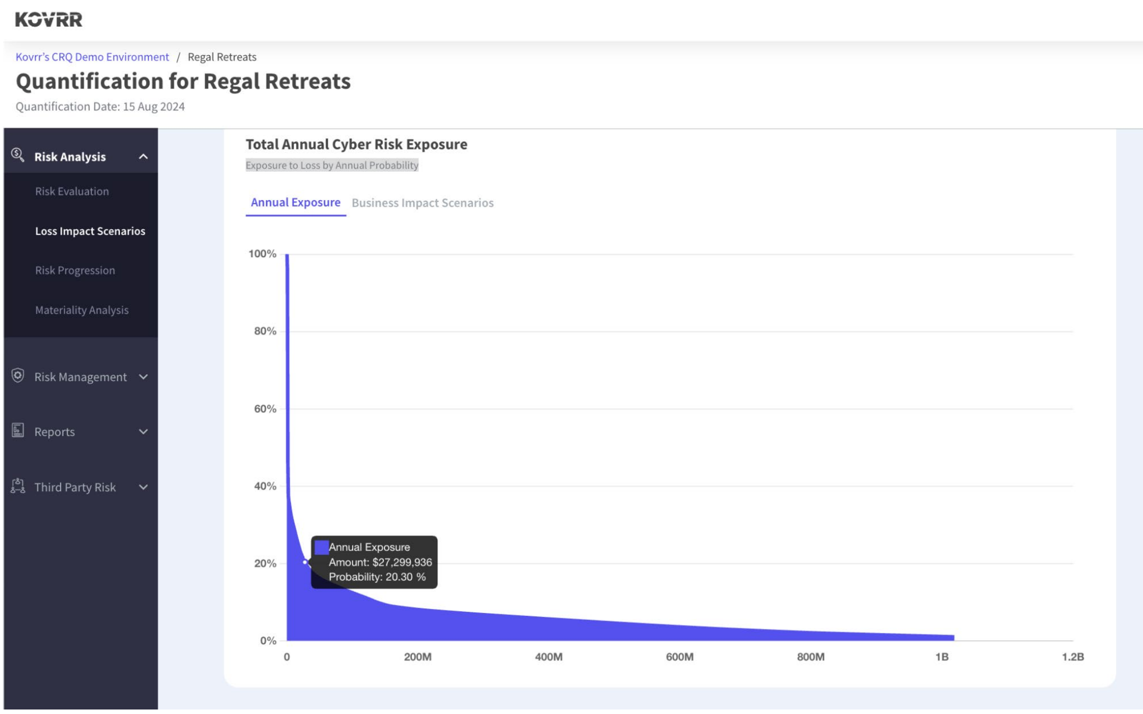
If, for instance, a modeled ransomware scenario shows a $2.3 million annual loss exposure and a proposed control reduces that by 60%, it becomes easier to justify that investment based on risk-adjusted terms. Whether CISOs or SRMs need to justify budgets or foster a broader understanding of cyber risk across the organization, Kovrr's platform provides the necessary foundational intelligence.

Building Strategic Maturity Through CRQ Iterations

However, these initial outputs are just the starting point, serving as the foundation for expansion. After the first quantification run, organizations can begin extending their CRQ efforts across different business units, integrating results into cyber risk registers and ongoing governance activities. Over time, teams can track residual risk reduction and align appetite thresholds with modeled exposure levels.

In another example, a board may eventually decide that no risk with more than a 10% chance of exceeding a $5 million loss should be tolerated. That level of clarity is only possible through quantitative modeling, and with each new iteration, the organization gets sharper and, therefore, better prepared for navigating the cyber threat landscape.

Interpreting the Loss Exceedance Curve



The loss exceedance curve illuminates a range of possible loss scenarios an organization faces.

A loss exceedance curve (LEC) is a staple output of the Monte Carlo simulations, illustrating the likelihood of experiencing a loss that reaches or exceeds a given financial threshold within the upcoming year, much in the same way a flood forecast shows how high water could rise if a storm hits. In the figure above, for instance, the simulation found that the company, Regal Retreats, faces roughly a 20% probability of losing upwards of $27 million in the next year.

The curve helps stakeholders visualize the full distribution of these potential monetary loss scenarios, from the most likely events to the high-severity, low-probability tail risks, allowing them to make more informed decisions regarding risk appetite levels, capital reserves, and cyber insurance limits and premiums.

On top of the core financial loss LECs, one highlighting average loss and the other breaking that loss down according to different scenarios, Kovrr's platform also offers exceedance curves for outage durations and the number of compromised records. These additional LECs provide CISOs and SRMs with a more holistic understanding of the operational implications of their organization's cyber risk exposure.

Specifically for one CISO at an Australian investment firm, Kovrr's financial LEC highlighted a tail-risk scenario that helped him to justify a multi-year uplift strategy focused on improving control maturity, eventually contributing to a 50% drop in the overall incident rate.

Institutionalizing CRQ for Long-Term Impact

As organizations gain experience in interpreting these outputs, the next natural step is institutionalization, which means embedding CRQ into regular risk assessments, investment planning cycles, control evaluations, and executive reporting. Once CRQ is firmly integrated into routine processes, cybersecurity leaders can build standardized reporting formats that include the loss exceedance curves, ROI estimates, and risk reduction trend lines, giving stakeholders a consistent, data-driven lens on cyber risk exposure.

Some companies will also opt to establish a dedicated team to steward the quantification process, ensuring that it's not merely a one-off analysis but a sustained capability supporting the organization's broader risk posture and maturity.

Why Leading Enterprises Choose Kovrr for CRQ

While numerous CRQ approaches and platforms exist, few, if any, deliver the level of precision and transparency required by today's enterprise-level stakeholders. Kovrr's platform distinguishes itself through an easy-to-use cyber risk modeling process and real-time threat intelligence data that builds confidence in security teams and executive leadership alike. Our solution, designed for both technical depth and executive clarity, ensures cyber risk management is treated as a core business consideration.

1. **Modeling Excellence:** Kovrr provides the only solution on the market that employs a multi-model approach (catastrophe and targeted) combined with a top-down modeling methodology for CRQ.
2. **Unique Data:** Kovrr's extensive data curation pipeline integrates a diverse range of continuously updated sources, including privileged insurance claims, and is regularly validated and calibrated.
3. **MITRE ATT&CK Scenarios Modeling**: Our solution offers out-of-the-box reporting, including automated calculations of severity and probability, aligned with the standardized MITRE ATT&CK framework.

4. **Root Cause Analysis:** Organizations have access to an automated root cause analysis, detecting potential deviations between quantification runs, such as a new prevalent CVE or a change in assets.
5. **Automated Materiality Thresholds:** Kovrr offers a unique-to-market analysis of an enterprise's "material" or "significant" cyber risks, developed to help organizations align with regulatory requirements, such as NIS2, DORA, or the US SEC's regulations.
6. **Integrated, CRQ-Powered Risk Register:** Powered directly by quantified insights, Kovrr's cyber risk register assesses the potential severity and probability of various loss scenarios. Sign up today.
7. **Bespoke Loss Distribution:** The platform fully supports the addition of specific loss distributions, allowing users to incorporate organization-specific data into the quantification process.
8. **Full Portfolio Risk Aggregation Analysis:** Kovrr's CRQ models provide a comprehensive portfolio analysis across all quantified business assets and can quantify these various risk exposures in the aggregate.

Putting CRQ to Work

With the power to bridge the gap between the more technical side of cyber risk management and high-level strategization, an on-demand cyber risk quantification (CRQ) solution has become an essential tool for organizations of all sizes. Kovrr's CRQ empowers CISOs and SRMs to transcend assumptions and, instead, harness measurable data to make key business decisions.

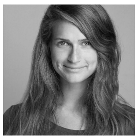
This advancement marks a stark turning point in the market, where cyber risk is no longer obscured by overly technical or vague terms but, rather, understood as a significant factor in enterprise performance. Against a background of escalating cyber events and mounting regulatory pressure, this alignment has become essential to building resilience at scale.

TO FURTHER EXPLORE how Kovrr's on-demand CRQ platform can support your organization in exposure mitigation and resiliency building, schedule a free demo with one of our cyber risk management experts today.

CONTRIBUTORS:

YAKIR GOLAN
Co-founder and CEO, Kovrr

DR. JACK FREUND
Kovrr Advisory Board Member



HANNAH YACKNIN – DAWSON Marketing Content Writer, Kovrr