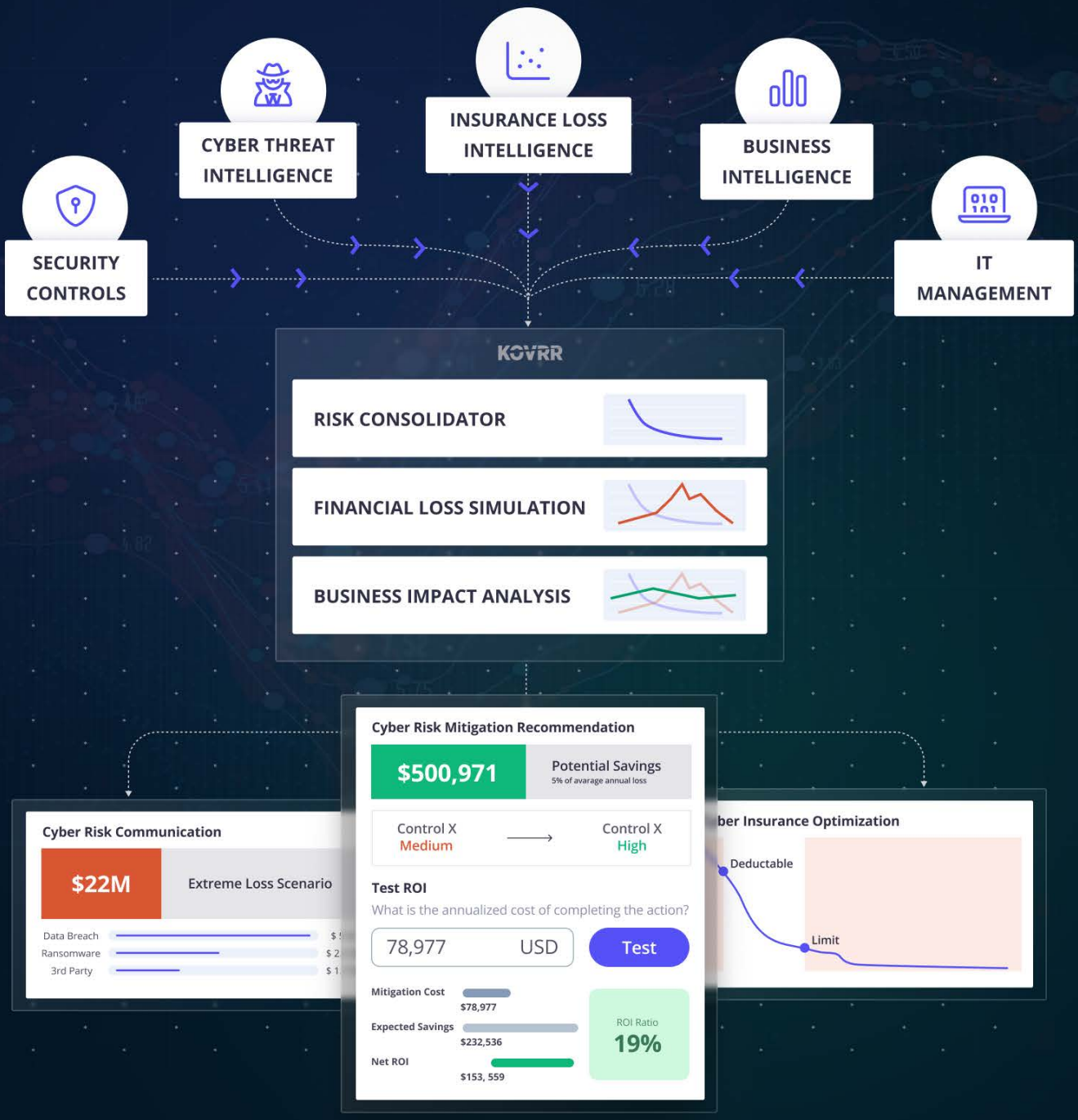
KOVRR



Kovrr's Cyber Risk Quantification Platform

Cyber Decisions. Financially Quantified.

Spearheading the CRQ revolution and Shift Up strategy, delivering on-demand financially quantified cyber insights with unmatched granularity.

Kovrr's cyber risk quantification platform empowers enterprise decision-makers to manage cyber exposure more effectively by providing an in-depth risk analysis that drives actionable, financially justified decisions that align with broader business goals.

Regardless of an organization's current framework, model, or risk register, Kovrr leverages the data and elevates the relative level of insight. Our enterprise-ready solution offers security teams a more granular, on-demand risk assessment that's communicable at the highest organizational levels.

Employing advanced cyber risk models and technologies trusted by cyber insurers and reinsurers worldwide, the platform shifts complex cybersecurity data into understandable financially-driven insights. Harnessing our exclusive access to large-scale insurance data and offerings, Kovrr's models are continuously validated based on data from millions of global companies.

Kovrr's data-driven approach is built from the ground up, facilitating objective, frictionless, and ever-evolving financial cyber risk quantifications that offer key stakeholders, including CISOs, CROs, board members, and investors, the necessary answers to circumvent significant financial losses and enhance resiliency.

Kovrr's powerful CRQ models lay the framework for business leaders to balance enterprise risk appetite, transfer, and mitigation activities. Shifting strategic cybersecurity discussions up to the top levels of an organization ensures optimal ROI on cyber investments while simultaneously reducing business vulnerabilities to cyber attacks and third-party service provider failures.

Shift Up: Elevate Cyber Risk Management Strategies

Communicate Cyber Risk in Financial Terms

Streamline decision-making by translating cyber risk into financial terms for the board and C-suite.

Measure Cybersecurity Program ROI

Assess a security program's ROI based on various risk mitigation efforts and prioritize investments to minimize the potential impact.

Optimize Cyber Insurance Policies

Identify gaps between risk mitigation options and insurance spending to create the optimal coverage plan.

Analyze Exposure From 3rd-Party Vendors

Gain crucial insights into 3rd and 4th-party vendors and financially quantify risks throughout the entire supply chain.

Meet Governance and Regulatory Standards

Strategically align cybersecurity and business goals. Adhere to reporting laws like those from the US SEC and APRA.

Conduct Cyber Due Diligence

Evaluate the cyber risk exposure of potential mergers and acquisitions, encouraging more strategic business decisions.

Seamless Integrations for Sharper Insights

Data integrations provide significantly improved visibility into cyber risk assets and vulnerabilities and ensure consistent, accurate information across various systems. Reduce manual data entry and subjective evaluations with seamless API integrations from Kovrr and make highly informed decisions based on a single source of truth.

Our cyber risk quantification solution integrates with multiple types of 3rd-party systems and platforms, including:

- Asset and Vulnerability Management
- CMDB (Configuration Management Database)
- EDR (Endpoint Detection and Response)
- GRC (Governance, Risk, Compliance)
- SOAR (Security Orchestration, Automation, and Response)
- BAS (Breach and Attack Simulation)
- IPS (Identity Provisioning Service)

TRUSTED BY ENTERPRISES WORLDWIDE

Royal Mail · LINKGroup · Allianz · MS&AD Holdings · AON · Mine · BRENTWOOD ASSOCIATES · playtech SOURCE OF SUCCESS · moodle · Bystronic · challenger · CHECK POINT

Why Manage Cyber Risk With Quantification by Kovrr?

In-Depth On-Demand Risk Overview

Eliminate reliance on slow, resource-invasive processes. Kovrr's cyber risk quantification models deliver insights such as top risk drivers and the largest contributions to cybersecurity programs.

Multi-Level Business Evaluation

Perform cyber risk quantification at any granularity level, including the group, subsidiary, and business units. Evaluate respective individual assets while maintaining a holistic view of the entire organization.

Continuous Quantification Insights Using Integrations

Harness all relevant enterprise security data from existing tools and frameworks via seamless API integrations or secure data export mechanisms to obtain a comprehensive, accurate CRQ view.

Business Resiliency With a Shift Up Strategy

Elevate cybersecurity management to the C-suite of executives and board of directors to ensure resources are effectively allocated in a cohesive, proactive manner that reflects the ever-evolving cyber risk landscape.

Most Significant Cyber Risk Identification and Prioritization

Discover which cyber events are most likely to cause significant financial damage and prioritize risk mitigation efforts accordingly. Minimize the impact of a cyber event before it ever occurs.

Insurance-Grade Cyber Risk Models

Leverage Kovrr's extensive database of loss data sources, including cyber insurance claims. Our models are validated at scale to highlight specific events that might impact your business.

Risk Mitigation Recommendations

Get actionable, financially quantified risk mitigation recommendations in alignment with the most prevalent risk frameworks, such as NIST, CIS, and ISO, offering detailed investment prioritization options. Explore insights into which controls contribute most to reducing overall exposure.

Industry-Specific Peer Benchmarks

Quantitatively gauge cyber risk exposure compared to peers and players in respective industries. Benchmark results between different business entities in a consistently measurable way.

Risk Models Adapted to Specific Business

Evaluate cyber posture according to an extensive, automatically-generated event catalog that matches the enterprise's technographic profile, associated 3rd-party providers, and relevant cyber attacks within the industry.

Ongoing Cyber Threat Intelligence

Analyze the enterprise's evolving risk scenarios, factoring in the latest global cyber events. Kovrr constantly updates the frequency and severity distributions to ensure the most accurate modeling of potential financial impact.

Material Cyber Event and Risk Reporting

Sharply define what qualifies as a material risk or event, fostering communication with legal counsel and the board of directors and facilitating mandatory disclosure and reporting processes.