VISIBLERISK a BitSight company

Reimagining Cyber Risk Quantification

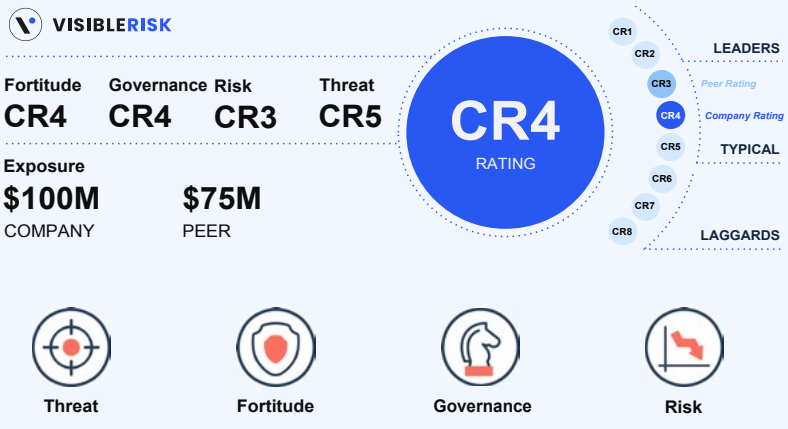
For Better Cyber Risk Management

Cyber security and cyber risk management are having a moment and it's not going to pass. Historically treated as technology problems for the CISO and security teams to handle, cyber security events are dominating the headlines today—and executives, media, and government agencies are taking notice. As the range and frequency of cyber security attacks increase, one question remains the same: how will this impact my business? This is where Cyber Risk Quantification (CRQ) comes in.

CRQ: Cyber Risk Quantification

What We Do

The VisibleRisk™ next gen cyber risk quantification platform translates cyber risk into financial terms the entire executive team, from the CISO to the board, can discuss. Unlike traditional cyber risk assessments that stop at the security control level and early CRQ practices that place a heavy lift on organizations, our solution incorporates critical business context in your cyber risk analysis while reducing workload through automated data collection, analysis and executive reporting. Our solution provides simplified output using an easy to understand rating scale, combined with economic analysis for board communication and all the underlying details that CISOs need to take action.



How it Works

We've created an automated and transparent approach that streamlines and expedites data collection, analysis and reporting so security leaders can reduce risk with greater accuracy and executives can make better business decisions around cyber risk with greater confidence.

1. Automated & Validated Data Collection

When it comes to data collection, we use data collector and tester tools to automate as much as we can and collect data from more sources than traditional audit tools, because we believe efficiency and validation are critical to cybersecurity. Our entire data collection process takes approximately a week and provides a robust and validated cyber risk assessment.

Direct Data - We go behind the firewall using APIs to collect data directly from existing security and technology systems while employing proprietary tester tools that simulate attacker capabilities and further enhance our risk model

Cyber Security Data - We partner with leading vendors in the security ratings, attack surface management and threat intelligence space in order to build a comprehensive view of your organization and eliminate the false positives so we don't conflate risk

Self Provided Data - We can consume pre-existing reports directly from security and technology management platforms or from prior assessment work and we validate the results of these reports before including them in our modeling

Management Dialogue - We engage in an active dialog with security and business leaders via a standard question set and interviews to gain an understanding of how the organization and management approaches cyber security to enhance our scoring of governance

External Business Profile and Loss Data - We leverage business profile information from Moody's data sets and other ratings research in order to set a baseline for our economic analysis. We further enhance this analysis by collecting loss information from commercial and open source data sets and then combine those data points with proprietary insurance claims data as well as information we collect directly from individual companies during an engagement

Receive a high fidelity, unbiased perspective of your security posture, with little effort.

This blended approach combines the view of multiple data sources with our own internal signals collection providing a holistic risk model that is unique in its ability to provide high fidelity results with relatively low effort.

2. Analysis and Modeling

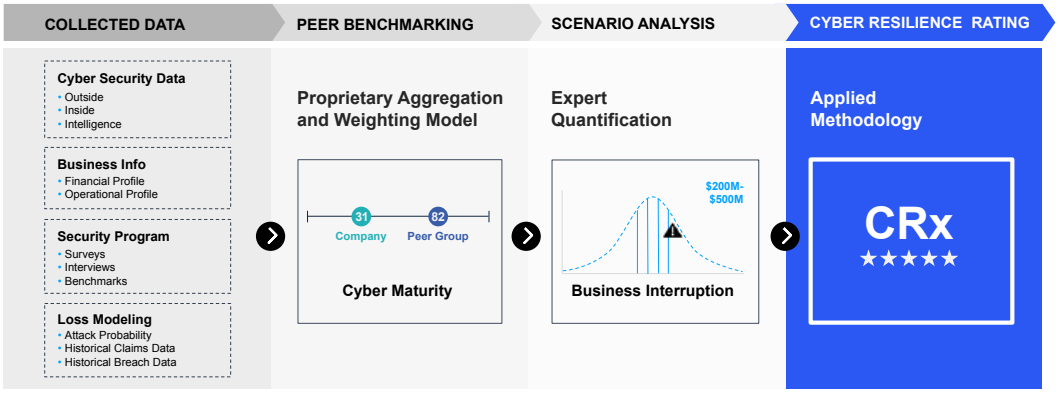
We go beyond traditional CRQ analysis to provide a more holistic, accurate and transparent perspective by incorporating a broader data set and providing complete visibility into our modeling. The VisibleRisk loss modeling consists of four scoring pillars: Threat, Governance, Fortitude & Risk.

The Threat pillar covers the current state of threat activity facing the organization.

The Governance pillar covers the areas where an organization's oversight and administration of security come into play (including elements of budgeting, resource management, strategy, and culture).

The Fortitude pillar encapsulates the ability of the organization to present a strong security posture to its threat communities (protection, detection, & resilience in the event of an attack).

The Risk pillar evaluates how financially material a cyber event or successful attack would be to the organization, and if they have the right insurance and capitalization to withstand a worse-case cyber incident.



VisibleRisk's methodology was developed and is overseen and constantly optimized by the co-author of the book on Open FAIR. While our methodology is based on Open FAIR, we've enhanced it to incorporate peer benchmarking and industry comparative losses, more objective scoring and provide custom insights and remediation actions related to your specific security posture.

Make confident, risk based decisions with more accurate modeling.

Our loss quantification methods are more objective because they are based on validated actual loss data compiled over thousands of events. This actuarial approach yields more accurate results than other approaches that rely on subject matter expert estimation.

3. Clear & Concise Reporting

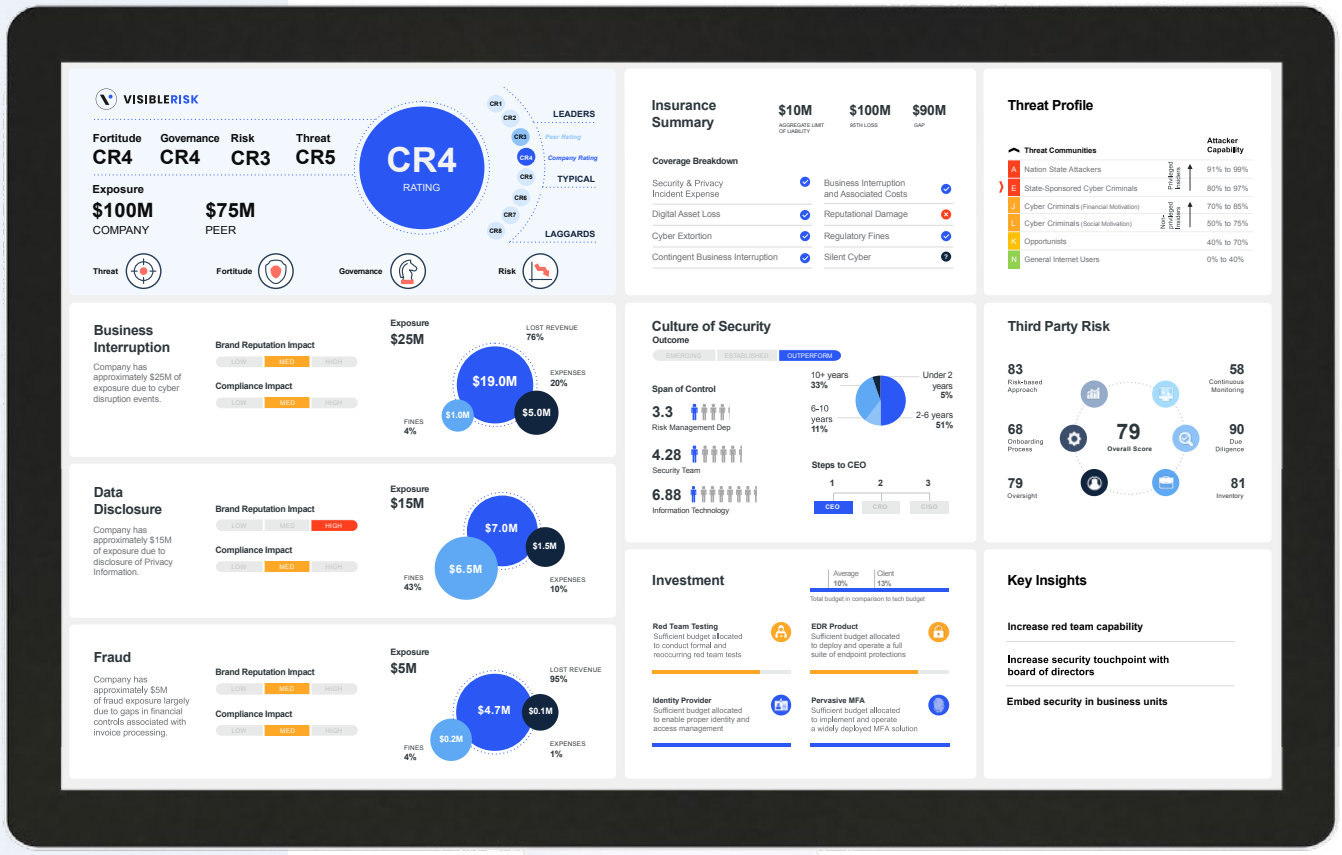
Our CRQ engine translates your cyber risk into financial terms, provides industry benchmarks, and presents them in a clear and succinct dashboard format that you can easily share with and present to your board. This includes:

An annual Cyber Resilience Rating presented where all organizations are rated on the same continuum of ratings from 1 (best) to 8 (worst) that reflects an organization's ability to withstand the potential cyber events that are likely to occur while maintaining their current state of financial stability & operation.

A dynamic cyber resilience dashboard that features multiple cyber resilience tiles to choose from and provides peer benchmarking and comparability insights

A downloadable cyber resilience report with includes additional risk quantification measurements and supporting details.

A cyber risk quantification analyst who sits in the middle of all the stakeholders to present the results and ensure a common understanding



4. Communicate & Act

Evolving your risk management methodology from traditional assessments to cyber risk quantification enables better communication and decision making from board reporting and security program optimization, to M&A, to insurance underwriting and limits considerations.

	**Board & executive reporting**	**Program optimization & budget allocation**	
	**Cyber insurance underwriting & limits adequacy**	**Mergers & acquisitions**	
	**Cyber risk assessments & Cyber risk quantification**	**Operational risk planning & Regulatory compliance**	

Sajan Gautam,
Chief Information Security Officer (CISO) at Arvest Bank

"VisibleRisk's cyber risk quantification platform helped me communicate critical aspects of our security program strategy to executives, raising both awareness of and support for our program."

Make better cyber risk management decisions.

Traditional cyber risk assessments do not translate cyber risk into business risk, making it difficult to communicate the benefits of a strong security posture or justify the need for more resources. By translating risk into business terms, the VisibleRisk CRQ platform enables better communication among all executive stakeholders. And thanks to a methodology rooted in transparency and validation, stakeholders can feel confident in their risk management decisions.

VISIBLERISK
a BitSight company

To learn more visit www.visiblerisk.com