Cybersecurity Risk Ratings:

A Feature, NOT the Full Picture in Cyber Risk Management

> Know the difference between risk ratings and risk quantification. A risk rating is not a quantitative measure of risk — full stop. Instead, it is a score based on security indicators that correlate with risk.
>
> ***The Forrester Wave™: Cybersecurity Risk Ratings Platforms, Q2 2024***

The Shift in Cybersecurity Perspectives

The recent Forrester Wave report on Cybersecurity Risk Ratings Platforms underscores a significant shift in the cybersecurity industry, advocating for a deeper understanding of risk ratings versus risk quantification. This distinction is not just semantic; it is foundational to how organizations should approach cyber risk management. As noted by Forrester, while risk ratings provide a score based on security indicators, risk quantification delves into the probability and material impact of risk scenarios, offering a more nuanced view of potential vulnerabilities and threats.

Risk ratings provide a score that reflects the presence or absence of risk indicators, which only suggests the likelihood of risk. These ratings are valuable for initial assessments and prioritizations but fall short in predicting the actual impact or probability of an incident. This limitation is particularly critical when making strategic decisions or investments in cybersecurity, where understanding the financial and operational implications of risks is crucial.

> Cyber risk quantification (CRQ) directly measures the probability and material impact of a risk scenario. They are related, and ratings data can be used in a CRQ analysis, but they are not the same.
>
> ***The Forrester Wave™: Cybersecurity Risk Ratings Platforms, Q2 2024***

Aspect	Cyber Risk Ratings	Third-Party Cyber Risk Quantification
Focus	Primarily focuses on likelihood indicators of risk without direct measurement of impact.	Directly measures both the likelihood and the material impact (financial) of potential risk scenarios.
Output	Scores or ratings that suggest general risk levels based on observed security controls.	Detailed financial metrics that estimate potential losses from specific cyber events.
Use Case	Useful for initial prioritization and identifying potential risk areas.	Critical for making informed, strategic decisions about cybersecurity investments and resource allocation.
Data Utilization	Uses static data points to generate a snapshot of risk based on current security controls and vulnerabilities.	Integrates dynamic, real-time data to continuously assess risk and update assessments as the threat landscape changes.
Stakeholder Communication	Provides a simple, easy-to-understand rating system for general awareness.	Delivers detailed, financially quantified risk assessments for precise and strategic business planning.
Strategic Value	Offers a baseline understanding of security posture; limited in driving strategic decisions.	Enables risk-based decision-making with detailed impact analysis, supporting strategic planning and risk transfer (e.g., insurance).
Scalability	Scalable for wide coverage but may lack depth in specific risk areas.	Highly scalable with depth, providing specific insights tailored to various business units and risk scenarios.
Business Alignment	Limited direct business impact assessment; very basic for board reporting.	Aligns closely with business objectives by translating cyber risks into business impacts and costs.