BLACK KITE

SOLUTION BRIEF

CYBER RISK QUANTIFICATION (CRQ)

Calculating the Financial Impact of Cyber Risk with Black Kite

You Can't Prioritize What You Can't Price

Boards hear endless cyber briefings, but what really resonates is understanding that a breach with a specific vendor could cost the organization $30 million. Without a common language to translate vendor exposure into business impact, the language of money, it is nearly impossible to rally stakeholders around prioritizing security actions.

The future of decision making is financial.

While technical data remains foundational, risk decisions from onboarding to insurance are increasingly evaluated through the lens of probable financial loss.

Black Kite's Cyber Risk Quantification (CRQ) solution turns vendor risk into a clear business conversation, empowering organizations to instantly weigh risk versus revenue.

Quantifying Cyber Risk With Black Kite

Black Kite's Cyber Risk Quantification (CRQ) solution is based on the **Open FAIR™ methodology** - the international gold standard for estimating the probable financial impact of cyber risk.

Key Benefits

- **Targeted vendor outreach and remediation**
- **Justify TPCRM spend and demonstrate program success**
- **Objective vendor comparisons using a consistent financial risk language**
- **Align security, finance, and leadership on risk tolerance**

Learn more about Cyber Risk Quantification (CRQ).

SOLUTION BRIEF

CRQ Solution Highlights

Scenario-Based Financial Impact Calculations

Black Kite automatically estimates probable financial impact across key risk scenarios, including ransomware, data breach, and business interruption.

Based on Open FAIR™

Built on the only international standard Value at Risk (VaR) model for cyber security and operational risk and optimized with business-specific context about your unique exposure.

Fully Automated

Never start with a blank model. Open FAIR™ factors are automatically populated using continuous monitoring data, assessment responses, and uploaded documentation.

Financial Risk Trends

Track how a vendor's financial risk changes by comparing real-time CRQ from continuous monitoring and point-in-time CRQ calculated as part of the assessment workflow to get a high-level understanding of potential financial impact over time.

What CRQ Enables

EXECUTIVE & BOARD RISK COMMUNICATION

Translate technical scores into financial exposure grounded in the internally recognized and trusted Open FAIR™ methodology to clearly communicate risk to non-technical stakeholders.

VENDOR OUTREACH & REMEDIATION PRIORITIZATION

Prioritize remediation efforts and campaigns to focus on the vendors that pose the greatest potential financial impact to your business.

DEMONSTRATED PROGRAM SUCCESS

Demonstrate how past TPCRM investments such as remediation campaigns have reduced overall financial exposure.

VENDOR COMPARISONS & NEGOTIATIONS

Use a consistent financial risk language to objectively compare vendors, guide selection, and strengthen renewal negotiations.

"While technical data will remain foundational, we see the future of third-party risk management being led by financial risk, which will become the key metric for decision making, increasingly shaped by board-level expectations"

CHUCK SCHAUBER, CHIEF PRODUCT OFFICER, BLACK KITE

Black Kite is a leading third-party cyber risk management platform trusted by thousands of customers to manage every supplier and every risk across their extended ecosystem.
To learn more, visit: www.blackkite.com

Gartner Peer Insights. Customer First

IT Vendor Risk Management Solutions

4.8 ★★★★★