Battlecard for CISOs: Pitching the Case for Cyber Risk Quantification and Management (CRQM)

SAFE

WHAT IS CYBER RISK QUANTIFICATION?

CRQ is a new approach to Cyber Risk Management. It applies risk quantification techniques to cybersecurity risk management - similar to credit scoring in financial services - to enable firms to assess, prioritize, and manage risk.

Unlike existing cyber risk management practices:

1. It integrates cyber risk with enterprise risk management.
2. It translates technical data into financial impact.
3. It is designed to help you identify and prioritize your most critical risk.

WHAT A LEADING CRQM PRODUCT DOES

- **Provides automated, continuous assessment and reporting** of enterprise-wide cybersecurity risk.
- Unifies cybersecurity platforms and datapoints within **a single dashboard to measure 360° posture.**
- **Assesses and monitors your entire attack surface** against security intelligence data, regulatory frameworks, and security standards..
- **Generates board-ready reports** that improve transparency and understanding during boardroom conversations.

PAINPOINTS & TRIGGERS	HOW CRQM SOLVES THE PROBLEM
I want to **understand my cyber risk exposure** across my attack surface	Quantify risk introduced by employees, processes, technologies, and vendors to **deliver 360° visibility of your enterprise risk**, rated by criticality, to help you reduce the likelihood of a breach.
I am concerned about the **security of my workload on public clouds**	Proactively manage the real-time risk of specific workloads **by categorizing assets according to your particular requirements.**
I need a **measurable way to assess and manage** my cyber risk	Report cyber risk using **a real-time risk score**: an objective output generated using API-driven inputs and data science. Leverage **an accountable, transparent method** to assess, prioritize, and manage cyber risk.
I am **unable to report cyber risk effectively** to the Board/Business Groups	CRQM platforms **translate technical data into business insights.** Security teams become better equipped to communicate risk and requirements with context to the business.
I need to **demonstrate the ROI** of my cybersecurity investments	Use quantification to measure your level of risk over time. Understand **which investments make the most positive impact** to your organization according to its geography, industry, and size.

COST OF NOT QUANTIFYING RISK

- **Not knowing the impact** of your security investments, or **underinvesting.**
- **Spending finite time and resources** addressing the least critical risk.
- **Missing critical risks** due to **point-in-time** assessments in an evolving threat landscape.
- **Poor, incomplete visibility** of your cybersecurity risk posture.
- No metric to hold the security team, business groups, and the Board **accountable**.

RETURN ON INVESTMENT

- **Predict your Breach Likelihood:** The probability of an attack within the next 12 months.
- **Calculates your $ value impact:** the potential financial impact of a breach.
- **Automatically Identify vulnerabilities** and generate the countermeasures to fix them.
- **Enhance the ability** of your security team to accept, mitigate, and transfer risk effectively.
- **Secure better cyber insurance coverage** at fairer premiums.

INDUSTRY ANALYST PERSPECTIVE

*"Cyber Risk Quantification will fundamentally revolutionize the way that **security leaders engage with boards and executives to discuss cybersecurity**"* - Forrester, 2022

*"When you can quantify cyber risks, you can better prioritize and protect new products, and push them to market more quickly. **That makes CRQ a critical part of your digital growth strategy**"* - Harvard Business Review, 2022

Battlecard for CISOs: Pitching the Case for Cyber Risk Quantification and Management (CRQM)

SAFE

OBJECTION HANDLING

POTENTIAL OBJECTIONS	HOW YOU CAN ANSWER THEM
You already have resources for measuring risk, **why do you need a platform**?	A quality CRQM product **automates measurement *and* management** processes to provide a living, breathing measurement of risk, as opposed to a manual, time-consuming, point-in-time assessment. It frees up the vital **time** of your **people** and deduplicates **technology** processes leading to greater **savings**.
How do you ensure quality when data is scattered across different products/teams?	Subjective, point-in-time inputs such as risk scenarios do not yield credible and objective outputs. With CRQM platforms, **input quality is controlled through automatically assimilated signals** from across your technology stack.
There's a cost to the platform - **how will it improve our bottom line**?	- **Deduplication:** Identifies overlapping or redundant security investments, including cyber insurance. - **Time:** Runs continuously in the background and reports risk on-demand, in real-time. - **Employees:** Automates manual processes to perform critical tasks in seconds, vs. hours/weeks/months.
Where do you get the data for a cyber risk quantification function to actually work?	CRQM platforms use **telemetry data, attack-specific reports** from security and threat intelligence research, data breach investigations, **insurance claim reports** from leading cyber insurance firms**,** and **your business' internal reports**. Plus, it **accounts for attack probability** per your industry, geography, size, and revenue.
We already employ tried-and-tested questionnaires to meet assessment needs	Questionnaire-based assessments expire quickly when used as a point-in-time exercise. You must challenge their validity if they *do not* take input from your own environment. **CRQM uses internal AND external data to deliver accurate assessments** with the added benefit of prioritized, actionable countermeasures.

*"Faced with the healthcare industry's rigorous compliance requirements and the rising risks of cyber attacks, it became a top priority for me to get a real-time, data backed and continuous view of exactly **how secure my critical applications are storing, processing and managing Public Health Information**. Safe Security helped me achieve this using CRQ"*
– Amir P. Desai, CIO, Molina Healthcare

CRQM AND THE FAIR FRAMEWORK

FAIR is often (incorrectly) considered the only acceptable solution for CRQ, however:

- It not practical to implement and does not scale.
- It requires specialist training and a dedicated team.
- Inputs are subjective; risk scenarios are hyper granular.
- It does not answer the '*so what?*' of quantifying cyber risk.

An automated, API-first, CRQM platform overcomes these challenges.

CYBERSECURITY RISK RATINGS SOLUTIONS (SRS)

SRS solutions cannot be used to quantify risk. Unlike CRQM:

- They only assess outside-in risk, and neglect to consider the impact of inside-out risk on security posture. This could leave you wide open to attack, so **a combined approach is key.**
- SRS solutions score your risk, but do not provide guidance or countermeasures to help fix the problems.
- Typically, they do not map against regulatory frameworks or security standards.

ABOUT SAFE SECURITY

Safe Security is a global leader in Cyber Risk Quantification and Management (CRQM). Our API-first CRQM platform, SAFE, tells you what your most critical risks are, the risks to accept, manage, or transfer, and the potential financial impact of a cyber attack, across any vector in your business. **To learn more, email getintouch@safe.security, or visit https://www.safe.security.**