

Cyber Quant



Cyber Quant evaluates an organization's risk exposure with a comprehensive approach to quantifying cyber risks, evaluates the processes, technology, and workforce security practices, and recommends actions moving forward.

Cyber Quant provides a **strategic cyber risk dashboard** of your organization through its contextual risk assessment and integration capabilities to answer **4 key questions**:



Do you know which **security gaps pose the greatest risk** to your business?



How can my organization's unique **cyber threat landscape** be **incorporated into risk assessments**?



What is the **financial impact of security breaches** on your organization?



How do your business and security leaders **determine where to invest**?

CYBER QUANT'S VALUE PROPOSITION FOR KEY STAKEHOLDERS



- ✓ Oversee quantified **automated reporting** and **cyber risk data in real-time** via **dashboards**
- ✓ Easily conduct **ROI and "what-if" analyses** before any activity involving cyber risk



- ✓ Communicate **cyber risk in terms that are easily understood** across the business
- ✓ Maintain **visibility of cyber risk** with granularity by business asset, division, and technology stack levels



- ✓ **Quickly assess the cyber risks** of divestitures and M&A activities
- ✓ Provide **budget prioritization** guidance driven by quantified risk insights



- ✓ **Pre-assess qualification** for industry-standard certifications
- ✓ Leverage Cyber Quant **assessment's track record** to highlight the organization's **focus on cybersecurity and risk management**



- ✓ **Develop strategy** to address security gaps and **organization's risk posture** over time
- ✓ Adjust **IT and security roadmaps** based on **tangible gaps & maturity evaluations**

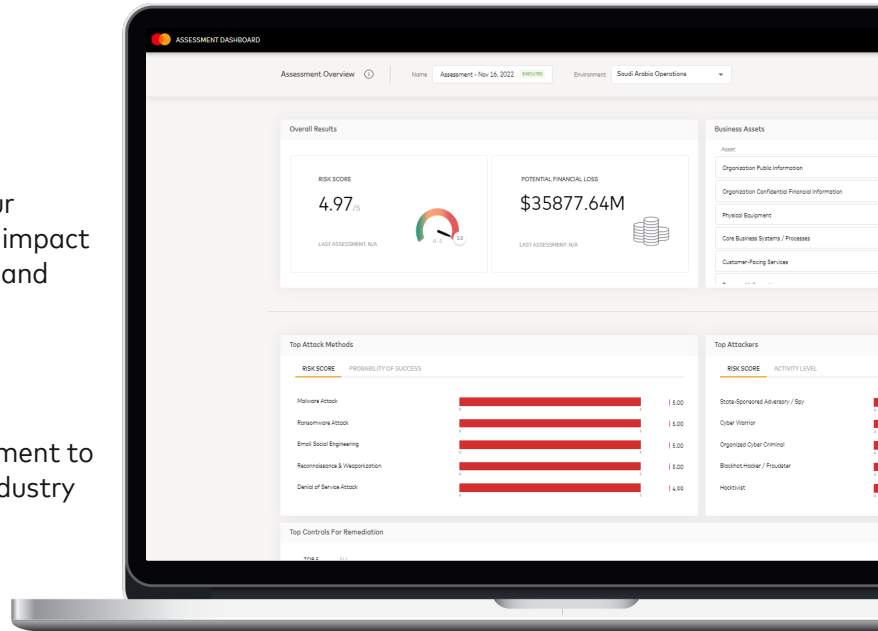
- ✓ Justify budgetary needs with **quantified ROI** and **"what-if" analyses**
- ✓ Utilize **quantified risk analytics** to evaluate **cyber insurance coverage**

HOW IT WORKS

With Cyber Quant, you can quickly take a highly automated and comprehensive approach to quantify cyber risks and potential financial loss

Cyber Quant utilizes a 4-step approach

- 1 Threat Landscape**
Evaluate demographic information about your organization to personalize threat landscape impact for your business based on location, industry, and organization size.
- 2 Questionnaires**
Analyze responses to customized, dynamic questionnaires to identify depth of risk, alignment to security standards and fit within other key industry framework.
- 3 Technical Analysis**
Validate your system's security settings alignment to your policies and industry best practices by securely evaluating 100+ technologies covering operating systems, cloud platforms, firewalls, security applications and more.
- 4 Evaluate & Act**
 - Automatically converge the information above to create role-based dashboards and reports
 - Calculate cyber risk score and financial impact of potential cyber events for your organization
 - Simulate scenarios to identify priority business and technical actions based on ROI from financial impact and risk reduction perspectives.



COMPETITIVE DIFFERENTIATION

Mastercard has unmatched expertise and extensive hands-on experience securing our own worldwide network



Security as a business model

Mastercard has **hands-on experience** protecting petabytes of its own data with the **Cyber Quant framework**



Personalized Insights

Mastercard **analyzes risks** taking into consideration the **threat landscape** specific to an organization



Dynamic Adjustment

Mastercard's methodology accounts for the **changing environment** of **cyber threats** and responds to **new attacks**