metricstream

EBOOK

POWER WHAT'S NEXT
BY MEASURING CYBER SECURITY RISKS

A DEEP-DIVE GUIDE INTO CYBER RISK QUANTIFICATION

TABLE OF CONTENTS

Introduction

CISOs, CIOs and IT security professionals are grappling with more cyber threats now than ever. From malware and ransomware, to DDoS attacks and zero-day exploits, the risks just keep increasing. So how do you know which risks to tackle first? Or where to focus your cybersecurity investments?

The traditional approach would be to rank all your risks as high, medium, and low. But these categorizations can be interpreted differently by different people. You might think a medium risk needs to be mitigated, but the management team might argue that it can be accepted. Defending your point of view can be tough because the term 'medium risk' sounds quite ambiguous.

It gets more challenging when you have 2-3 different risks that are all ranked medium. Which one do you focus on first? Do you spend the same amount of time and resources managing all three risks? It's difficult to know for sure.

But what if you were told that a malware attack on your organization could cost you $3 million in losses? And that there's a 60% chance of that loss occurring? Now, things become clearer, both for your IT security team and the business. You can quickly come up with a response, get consensus, and take action to protect your business.

What you've done is inject more accuracy and clarity into your cyber risk assessments. Ambiguous terms have been converted into hard numbers. And that can make all the difference.

81% of C-suite executives who quantify cyber risk say it has helped increase productivity and sharpen focus on strategic matters.

PwC's US Digital Trust Insights Snapshot 2021

ASSIGNING A DOLLAR VALUE TO RISK

What Is Cyber Risk Quantification?

Simply put, cyber risk quantification is the process of measuring IT and cyber risk exposure in monetary terms. It helps you determine which risks to focus on first, and where to allocate your cybersecurity resources for maximum impact.

Typically, **cyber risk quantification** uses sophisticated modeling techniques like Monte Carlo simulations to estimate the value at risk (VaR) or expected loss from risk exposure.

By quantifying the monetary impact of a risk event, you can confidently answer questions like "How much should we invest in cybersecurity?", "What will be the return on investment?", and "Do we have enough cyber insurance coverage?"

Risk quantification can benefit multiple stakeholders. CISOs gain a deeper understanding of risk impact which helps them make data-driven decisions. Boards have more visibility into what's at stake for the business in terms of dollar value. And executives can effectively prioritize cybersecurity investments, driving alignment between cyber programs and business goals.

> "Cyber risk quantification is now firmly established as a key innovation and indispensable value-add to integrated risk management and GRC. Organizations can make data-driven decisions based on risk exposure versus required investments. CISOs and CIOs can also communicate cyber risk exposure in financial terms to the C-suite. Security and risk professionals gain an efficient basis for allocating cyber security budgets and limited resources to prioritize mitigation efforts."
>
> **Bruce Dahlgren,**
> Chief Executive Officer, MetricStream

ANSWERING THE WHY

Reasons to Quantify Your Cyber Risks

Risk quantification isn't a new practice. But it's receiving more attention these days because of the following reasons.

Cyber-attacks are getting more complex and aggressive

The UN reported a 600% increase in malicious emails during the pandemic. Cisco predicts that DDoS attacks will touch 15.4 million by 2023. Cybersecurity Ventures estimates that cybercrime will cost the world $10.5 trillion annually by 2025. All this means that we need to get smarter about how we assess, measure, and respond to cyber risks.

Attack surfaces are expanding

Businesses are increasingly adopting AI, IoT, robotic process automation, cloud apps, and other digital technologies to achieve their business goals. But all that digitization creates more entry points for cyber criminals to breach sensitive networks. If we want to stay ahead, we have to build a more accurate understanding of risk impact and likelihood.

Cybersecurity budgets and resources are limited

Organizations face thousands of IT and cyber risks. The challenge is to figure out which risks to deal with first. Likewise, there may be hundreds of possible security controls. Which one will yield the most benefits for the least cost? These are questions that CISOs have to answer because their budgets are finite. Investments have to be allocated as efficiently as possible. That starts with quantifying the financial loss of a potential cyber risk. When you know how much the risk will cost you, and how much a particular control can help lower that cost, it becomes easier to decide where to direct security investments.

Qualitative measurements aren't always sufficient

Cyber risks have historically been communicated in qualitative terms like "probably likely to occur" or "somewhat likely to impact the business". But these terms often raise more questions than provide answers. What does "probably likely" mean? How is it different from "somewhat likely"? If resources are applied to a "probably likely" risk, how much risk reduction will be achieved? To answer these questions, we need more quantitative data.

> "It is clear that organizations need solutions that protect digital workers while rapidly addresing the digital transformation and thwarting off increased cyber threats. Cyber leaders are beginning to realize that resilience is only one step towards managing risk. An integrated risk management approach enables visibility to real-time data to quantify risk and make more strategic business decisions."
>
> **Gaurav Kapoor,**
> Chief Operating Officer and Co-Founder,
> MetricStream


MAKING THE MOVE
TO TOMORROW

Benefits of Quantifying Cyber Risk

By measuring and communicating cyber risks in monetary terms, you can:

Make better-informed decisions

No longer do you have to guess which IT and cyber risks to prioritize based simply on intuition or judgement. With properly quantified risk data, you understand the true impact and probability of a risk. You know where to focus your cyber investments, and how to reduce your risk exposure in line with business objectives. You're less likely to over-react or under-react to potential risk events. Instead, you're able to make calculated **IT and cyber risk management** decisions that yield optimal value.

Strengthen the objectivity and accuracy of your risk assessments

When you express cyber risk exposure in clear and precise terms, you minimize uncertainty. There's much less debate and confusion about what the top three cyber risks are, or why they've been ranked that way, or which controls are most relevant to mitigate those risks. The data is there for everyone to see.

Demystify cybersecurity for the board and management

Cybersecurity presentations to the board and leadership team can be filled with confusing technical jargon. Or, they fan the flames of FUD (fear, uncertainty, and doubt). But that doesn't help with effective business analysis or decision-making. Quantification, by contrast, provides a more nuanced and easy-to-comprehend view of cybersecurity risks. Boards and executives can quickly understand the most critical and costly cyber threats facing their business. CISOs, in turn, can better justify the need for cybersecurity investments.

Understand the effectiveness of risk mitigation strategies

When you invest in a security control, you want to know how effective it is. Cyber risk quantification can help you understand how much risk reduction has been achieved with each control. If you find your risk exposure is still high, you can quickly re-direct your investments to another, better control. This way, your cyber risk mitigation efforts become more proactive and productive.

Gain a competitive advantage

Cyber risk quantification helps you strengthen your cyber maturity and resilience. It gives you the insights to respond to cyber threats in a more targeted and cost-efficient way. That translates into improved customer trust and credibility. Companies using, or planning to use, quantitative risk assessment models are ahead in digital transformation, and have overall higher cybersecurity performance.

> "Over the past three decades we have seen the evolution of market risk, credit risk, and operational risk. Cyber risk quantification is a natural extension of the qualitative assessments that organizations have already been doing as the factors involved are the same. We're talking about the assets, the threats, the vulnerabilities, and the assessment of those vulnerabilities, and the controls that you have in place, to mitigate the risks and the losses."
>
> **Prasad Sabbineni,**
> Chief Technology Officer, MetricStream


MODELS AND
FRAMEWORKS

FAIR™ Model for Cyber Risk Quantification

Factor Analysis of Information Risk (FAIR™) is an international standard quantitative model framework to understand, analyze, and quantify cyber risks in financial terms.

With FAIR, you can quantify your security risk exposure in terms of the dollar value at risk. The framework helps you challenge and defend your risk decisions using an advanced risk model, while also determining how security investments will impact your risk profile.

FAIR can be used in tandem with other risk assessment frameworks such as NIST, ISO, and OCTAVE. While many of them rely on qualitative color charts or numerical weighted scales to assess risks, FAIR adds a quantitative dimension that makes risk assessments more holistic.

Other Frameworks to Assess Cyber Risks

- ISO 27005 acts as a guideline for information security risk assessments. It doesn't outline a specific methodology, but it does imply continuous risk management based on the following components: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review.
- NIST SP 800-53 was developed by the US National Institute of Standards and Technology (NIST) to establish common control assessment procedures for federal organizations. But many private organizations also use NIST to determine if their security controls are implemented correctly, operating as intended, and producing the desired outcome.
- OCTAVE or the Operationally Critical Threat, Asset, and Vulnerability Evaluation was developed by Carnegie Mellon University for the Department of Defense. The new version, OCTAVE FORTE, helps organizations evaluate their security risks, and use ERM principles to bridge the gap between executives and practitioners. OCTAVE Allegro – which serves as a complement to OCTAVE FORTE – helps streamline and optimize security risk assessments.
- COBIT® 5 was created by the Information Systems Audit and Control Association (ISACA) for enterprise IT governance. It enables a consistent and accurate assessment of IT risks and their impact on an organization.

Why Use Monte Carlo Simulation Models?

A Monte Carlo analysis is a powerful tool to help you model the probability and impact of different risk exposures in quantitative terms. It simulates a cyber risk event like a ransomware attack multiple times over, so that you can predict the financial losses that could result from each scenario – ranging from best-case, to most likely, to worst-case scenarios. Based on these insights, you can decide on the best approach to risk mitigation.


BEFORE
YOU START

Best Practices for Cyber Risk Quantification

While many of the risk assessment frameworks covered above provide clear guidelines and procedures on how to measure cyber risks, here are a few best practices to get you started:

- Build a comprehensive profile of your information assets. Know where they're stored, transported, and processed
- Identify the threats that could compromise the security and privacy of your assets. Determine which of these assets are most vulnerable to the identified threats
- Analyze the controls that are in place to minimize the probability of the threats or vulnerabilities
- Capture the financial consequences of a threat being realized. For instance, a data breach could result in multiple financial losses – be it legal liabilities, regulatory penalties, reputational costs, or customer damage claims. Use industry data or insights from past cybersecurity incidents within the organization to estimate the cost and scale of risk impact
- Determine the most likely loss outcomes using Monte Carlo simulation models
- Prioritize risks based on their financial impact and probability. Select a mitigation approach
- Document and report the results to help management decide on cybersecurity budgets, policies, and procedures

6 Things to Keep in Mind When Quantifying Cyber Risks

1. **Establish a common risk language:** If everyone in the organization has a different definition for IT asset, threat, or vulnerability, you'll find it difficult to communicate and defend your risk decisions. Standardize the risk nomenclature as much as possible.
2. **Involve other functions:** Cyber risk quantification is a collaborative exercise that goes beyond the IT security department. Engage other divisions in identifying critical risk scenarios. The more perspectives you have at the table, the more comprehensive your risk data will be.
3. **Revisit risk results periodically:** Cyber risks and threats are always evolving. A risk that was critical a year ago may not be so anymore. The only way to know is to re-quantify your risks at regular intervals – maybe once or twice annually.
4. **Start small:** It's neither efficient nor effective to cover all possible threats and risk scenarios at once. Pick one important use case and work on that first.
5. **Automate wherever possible:** Manual cyber risk quantification processes can be both complex and time-consuming. Find a solution that can help you automate workflows, and measure risks faster.
6. **Remember, quantification isn't a panacea:** Cyber risk quantification should enhance, not replace other IT and cyber risk management processes. Its value is best realized when complemented with risk monitoring, qualitative assessments, internal audits, and issue management processes.

HOW METRICSTREAM CAN HELP

The Cyber Risk Quantification framework from MetricStream is designed to enable you measure, manage, and report cyber risk in monetary value. As the first use case from MetricStream Intelligence—a new flexible analytics and AI engine that encompasses multiple calculation engines, AI/ML, and data science capabilities--MetricStream's Cyber Risk Quantification framework brings native capabilities for advanced Cyber Risk Quantification and Monte Carlo Simulation.

The framework is flexible to enable your organization to build homegrown models or adopt industry-standard models such as the FAIR model as well as other models. Presently, the FAIR (Factor Analysis of Information Risk) model is fast emerging as the standard methodology for cyber risk quantification and is widely recognized in the industry for calculating the value at risk for cybersecurity. With FAIR, asset-based risks can be quantified per their threat and vulnerability exposure leading to the calculation of the final dollar value at risk. In addition to supporting the FAIR model, MetricStream's Cyber Risk Quantification framework supports other methodologies like ISO 27005, NIST SP 800-53, CMU OCTAVE, and COBIT 5.

MetricStream's Advanced Quantification and Simulation enables users to build any kind of custom models, use various factors and variables, capture values for factors (e.g., threat event frequency) that are represented in a simple, parent-child hierarchal format. The accuracy of quantification can be further improved with a wide range of factors (e.g., Mix, Max, Most Likely, and confidence). Monte Carlo simulation can also be triggered by users to generate a range-based estimate and predict the probability of different outcomes for the Annual Loss Expectancy.

With MetricStream's Cyber Risk Quantification framework, your organization will be able to power what's next by equipping:

- Boards & executives to better comprehend cyber risk exposure by understanding what's at stake in dollar value
- Executive teams to prioritize cyber investments better, driving alignment between cyber programs and business goals, and plan for optimal insurance cover
- CISOs to be more accurate about the impact of cyber risks like data breaches, identity theft, infrastructure down time, etc.
- CISOs to develop a defensible justification for cyber investments, based on the risk quantification models' response to newer additional controls

No organization can ever be fully invulnerable to threats and risk – but smart risk management and measurement will keep you a step ahead.

metricstream

CONTACT US | REQUEST A DEMO

Email: info@metricstream.com