Making the Juice Worth the Squeeze

A Better Way to Quantify Cyber Risk - Faster, Leaner, Board-ready.

AS SEEN IN

Forbes yahoo!finance CYBER DEFENSE MAGAZINE Cybersecurity INSIDERS

Who This Paper Is For

This paper is written for **CISOs, Chief Risk Officers, and cybersecurity executives** responsible for aligning cyber risk with business priorities and communicating that risk in financial terms that resonate with Board-level stakeholders.

You may already be using a cyber risk quantification methodology such as FAIR. You've likely experienced the limits of these methods:

- The process takes too long.
- The inputs are difficult to defend.
- The results are too technical to guide strategic decisions.

This paper introduces a different approach, designed to help you quantify cyber risk at scale with lean inputs and clear business logic. It's built for those accountable for steering cybersecurity as an enterprise risk.

It's not FAIR.

If your job involves **reporting cyber risk to the Board**, **prioritizing security investments**, or **justifying cyber spend in financial terms**, this paper is for you.

Why Prevailing CRQ Methods Fail for Boardroom-Level Decision-Making

The Missing Link Between Technical Risk and Business Accountability

Cybersecurity has always had a translation problem. Technical teams talk about vulnerabilities and threats. Boards want to understand financial exposure and business impact.

As attacks grow more costly and regulators hold executives increasingly accountable, this gap is no longer sustainable.

Over the past decade, cyber risk quantification (CRQ) has gained traction. Quantification methodologies have matured to bring structure and numbers to risk. But the reality in most organizations still looks the same: spreadsheets, heatmaps, and educated guesswork.

In a 2025 PwC study, **88% of executives** said that "measuring cyber risk is crucial for prioritizing investments." Yet only **15%** said they were measuring the financial impact of cyber risks to a significant extent.

So what's causing the disconnect?

Security teams and decision-makers alike report frustrations with CRQ:

- The outputs miss the big picture view across a company
- The results don't reflect how the business sees risk
- Quantified assessments take too long to produce
- The process is complex and hard to repeat
- Inputs rely on data that doesn't exist or can't be trusted

In other words, while executive value quantified risk results, they perceive that the juice often isn't worth the squeeze.

That's a problem. Because the promise of CRQ - better decisions, smarter investments, clearer accountability - is still critical.

So, the question is: **Is there a different way to do CRQ**?

A Business-First Alternative to Technical Risk Models

Most traditional frameworks start from the bottom: modeling individual systems, threats, and controls. These technology-first models can provide detailed insights but scaling that detail to the enterprise level is slow, error-

prone, and resource-intensive: the further you zoom out, the more fragile the analysis becomes.

What's needed instead is a **business-first approach**, one that starts at the top with executive decision making in mind, frames risk in terms of financial exposure, and guides the Boardroom discussion without getting buried in system-level complexity.

This whitepaper introduces the approach of **Top-Down Cyber Risk Quantification**. It explores:

- Why traditional CRQ models fall short at the executive level
- How Squalify's top-down CRQ methodology works
- What makes this model different (and why most organizations can't replicate it)
- How top-down CRQ enables faster, clearer, and more strategic decisions.

If you're responsible for turning cyber risk into business decisions, this is where you start.

From Technical Systems to Business Scenarios

Reframing Cyber Risk as a Strategic Business Problem

Bottom-up Quantification: A System Level Analysis

One of the most widely used cyber risk quantification methods today is the **FAIR model (Factor Analysis of Information Risk)**. FAIR (and similar frameworks) start at the system level. They identify individual assets, assess potential threats to those assets, evaluate the controls in place, and then estimate the likelihood and impact of a successful cyber attack.

This logic can provide valuable insights for specific systems or applications. But it comes at a cost.

System-level models like FAIR:

- Rely on detailed technical data that's often incomplete, hard to validate, or unavailable
- Require time-intensive workshops to estimate threat event frequencies and control failure probabilities
- Are difficult to scale across complex business structures or multiple subsidiaries
- Produce detailed technical outputs but lack clear business relevance.

For many organizations, the result is a quantification effort that takes months to complete and still leaves Boardroom questions unanswered.

Top-Down Quantification: A Business-First Approach

By contrast, business-level CRQ takes the opposite approach.
Instead of asking:

"How likely is it that System X will be compromised by Threat Y?"

It asks:

"If this part of our business is hit by a serious cyber event, what's at stake?"

Because if you want to make cyber risk make sense to the Board, the logic needs to match how they already think about enterprise risk: financially, comparatively, and defensibly.

Top-down quantification starts by understanding how the company makes money, identifying the cyber scenarios that can threaten that business model, and finally considers how well those critical business functions are protected.

It reframes cyber risk as a strategic business issue and models the **financial consequences** of major cyber events in financial terms.

Top-down quantification enables cybersecurity teams to address Boardroom priorities using the financial language executives rely on, including questions like:

- What could a major cyber event actually cost us?
- Where is our biggest financial exposure?
- Are we spending too much—or too little—on cybersecurity?

"With the Squalify platform, we now have a clear view of which business scenarios could hit us hardest and how our cyber risk posture has shifted over the past 18 months. It's the first time I've been able to show my Executive Board, with confidence, that we're focused on the right threats and making measurable progress."

Brian Cook, Senior IT & Security Manager @Henry Meds

Why Top-Down CRQ Only Works with the Right Data

Because Without Real-world Loss Data, CRQ Is Just Guesswork.

Top-down cyber risk quantification depends on estimating the real financial consequences of major cyber events.

For this approach to work, it requires access to meaningful loss data: how often incidents are occurring, and what cyber incidents have actually cost companies in the past, across different sectors, regions, and sizes.

Most organizations don't have this kind of data. Public breach disclosures are limited, often incomplete, and focused on large headline events. Internal data from prior incidents is typically too narrow to inform forward-looking planning. This is where Squalify's foundation is different.

As a wholly owned venture of Munich Re, the world's leading cyber reinsurer, Squalify has exclusive access to one of the most comprehensive cyber loss databases in the world. This database was built over more than a decade through Munich Re's global cyber insurance activities.

It includes:

- Financial loss data from over 100,000 companies
- Covering 80+ countries and 130+ industries
- A wide range of event types: data breaches, ransomware, business interruption, third-party failures, financial fraud, and more
- Both direct costs (e.g. legal, recovery, regulatory penalties) and indirect consequences (e.g. operational downtime, customer churn, reputational damage)

What makes this database unique is that it reflects **actual cyber insurance claims paid** (not estimates or survey data). The incidents captured in this dataset include both public and non-public cases, giving a far more complete picture of real-world cyber exposure than is available anywhere else.

Through this dataset you no longer need to guesstimate threat event frequencies; instead you can focus on the costs to your company. Squalify delivers fast, repeatable cyber risk quantification that is concrete, explainable and aligned with how Boards evaluate other forms of enterprise risk.

How the Insurance Lens Makes Top-Down Models Possible

The Risk Model Behind 4,500+ Real-World CRQ Assessments

Squalify's top-down model comes from cyber insurance. It was developed at Munich Re, the world's leading reinsurer, to price cyber risk across thousands of global companies in high stakes underwriting decisions.

This same model is used today by Munich Re to underwrite billions in cyber policies. Therefore, estimating the financial impact of cyber risk isn't a theoretical exercise for Munich Re. It's a business-critical function. Misjudging the exposure of a company or a portfolio means taking on more risk than the premium can cover. If the model is wrong, Munich Re loses money. Period.

Instead of modeling individual threats to individual systems, insurers start with the question: **What would it cost this company if a severe cyber event disrupted its business?**

This is fundamentally different from most cyber risk practices inside organizations today. Internal teams typically start at the technical level, estimating likelihoods for threat scenarios tied to IT systems or processes.

These efforts often struggle to scale, because of the large number of systems to quantify, and the difficulty of combining individual risk assessments. Insurance-based thinking does the opposite:

- It **starts with financial impact**, using real-world loss distributions
- It **benchmarks exposure**, not just maturity or controls
- It **prioritizes consequences**, not individual vulnerabilities

This approach also inherently aggregates risk across **systems and technologies**, which makes it scalable across entire enterprises; even those with complex, decentralized infrastructures.

Squalify brings this logic into the enterprise. As a wholly owned Munich Re venture, we translate the portfolio-based view of cyber risk into a business-facing CRQ platform. It's built to help cyber-, risk-, and executive leaders use the same framing insurers use to evaluate financial exposure, only now applied internally, for proactive steering rather than insurance underwriting.

For you, this means you're using the same methodology trusted by the global insurance market. More than 4,500 companies have already been assessed using this methodology. It's embedded not just in the Squalify platform, but also in Munich Re risk assessments and major partnerships.

From Threat to Financial Loss: How the Model Organizes Risk

Squalify's risk model simulates the frequency and severity of cyber scenarios for each organization based on its individual profile.

To quantify cyber risk in financial terms, the Squalify Model follows a three-layer structure: from cause to consequence to cost:

1. Cyber Threats: What Could Happen

These are patterns of real-life cyber incidents. Each threat type is based on historic incident data and reflects the types of attacks that typically drive financial loss in the insurance market.

This threat modeling is built into the model (and regularly updated), so you do not need to estimate threat inputs.

2. Consequence Scenarios: What It Impacts

You'll assess three common types of cyber incidents based on your business model:

- Data Privacy Breach: sensitive data is exposed
- Business Interruption: operations are disrupted
- Theft & Fraud: funds or digital value are stolen

Ransomware is treated as a hybrid event, combining both data breach and business interruption scenarios.

3. Loss Components Quantified as Financial Loss Values

Each consequence drives specific financial impacts, grouped into seven Loss Components. These reflect actual cost categories seen in real cyber insurance claims. If you're familiar with the cost components in the FAIR Materiality Assessment Model (FAIR-MAM) you will be able to quickly adapt these to the Squalify Loss Components.

The model calculates potential costs across each component to produce quantifiable loss values. So you get financial numbers that hold up in the Boardroom.

Minimal Data Collection. Lean Input. Fast Results.

Top-down CRQ doesn't rely on technical data dumps or endless spreadsheets. It's designed to work with inputs that risk managers and CISOs already know or can quickly gather from existing reports.

The goal isn't to model every detail. It's to surface the financial relevance of cyber risk using high-leverage data that reflects your business reality.
The only inputs you need include:

Basic Exposure Data

This includes your company's:

- **Revenue** (overall financial footprint)
- **Industry** (to calibrate against sector-specific risk patterns)
- **Share of Personal Data Processed** (to determine privacy-related exposure)
- **Geographic Footprint** (to reflect regulatory and operational complexity)

Most of this data is readily available from annual reports, compliance documents, or basic company stats.

Scenario Descriptions

You'll assess three common types of cyber incidents (they cover more than 99% of all types of cyber incidents) based on your business model:

- **Business Interruption**
- **Data Privacy Breach**
- **Financial Theft or Fraud**

These scenarios don't require threat modeling. You are simply estimating how disruptive the consequences of each type of event would be to your operations. Think of it like assigning impact levels, something risk teams already do in other domains.

Information Security Maturity

A brief self-assessment across key cybersecurity domains. No deep-dive audits or control scoring. Just a high-level view of how established your current practices are based on what's already tracked in your information security management system (ISMS), or internal maturity reviews. This is security maturity at a company level, rather than individual system performance. Squalify uses the NIST CSF by default but can also map to your custom cybersecurity framework.

With just these inputs, a full enterprise quantification is possible, at a strategic level, within days and in financial terms.

It's not just faster. It's designed to match how the Board thinks about risk:
Business-first. Impact-focused. Decision-ready.

Conclusion: Making the Juice Worth the Squeeze

Most cybersecurity leaders don't need convincing that quantifying cyber risk is important.

The challenge has always been in the how: traditional methods take too long, rely on assumptions no one can defend, and still don't deliver what the Board needs.

Too often, quantification efforts remain stuck in technical detail, whether measuring threats to systems instead of consequences to the business or struggling to provide a big-picture view at a company level**.** The result is risk analysis that feels precise but lacks strategic relevance.

A **business-first**, top-down approach reframes the problem entirely. It starts not with infrastructure, but with impact. It reflects how companies operate, how they create value, and what they stand to lose in the face of a serious cyber event. This perspective doesn't just simplify the process; it reorients it around what executive leaders need to know.

When less effort delivers more clarity and when cyber risk finally speaks the language of the Board: that's when the juice becomes worth the squeeze.

About Squalify: Cyber Risk Quantification for the Boardroom

Squalify is a **cyber risk quantification platform for the Boardroom**. Our risk insights support information security and risk executives to answer the Board's toughest cybersecurity questions and steer group-wide risk reduction effectively from one platform. Fast. Data-backed. Scalable.

We are a corporate venture of Munich Re, one of the world's largest cyber reinsurers. Our proven risk model is built on a decade of cyber insurance expertise and powered by exclusive access to Munich Re's industry-leading cyber loss database; covering over 100,000 companies across 130+ industries and 80 countries. More than 4,500 companies have already been assessed using our quantification methodology.

- Want to see how this works in practice? Book a meeting
- Learn more on www.squalify.io
- Follow us on Linkedin
- See what Forbes is saying about us

AS SEEN IN

Forbes yahoo!finance CYBER DEFENSE MAGAZINE Cybersecurity INSIDERS