


EBOOK

Establishing a Universal Understanding of Cyber Risk With Financial Quantification



ESTABLISHING A UNIVERSAL UNDERSTANDING OF CYBER RISK WITH FINANCIAL QUANTIFICATION

The Need to Reshape the Cyber Risk Conversation	3
Quantifying Cyber Risk Using Proven Models Developed for Cyber Insurance	4
What types of data are incorporated into the quantification process?	6
How does multi-model analysis work?	7
What types of business insights does this multi-model approach provide?	9
How the BitSight Financial Quantification Empowers You to Mature Your Cybersecurity Program	10
1. Streamline your process for quantifying cyber risk	10
2. Make more informed business decisions	11
3. Report to the board effectively	11
Elevate Cyber Risk to Business Risk	12

THE NEED TO RESHAPE THE CYBER RISK CONVERSATION

To bridge the language gap between security and the business, cybersecurity leaders are turning towards analyzing cyber risk in the same way the organization looks at other issues: in terms of its financial impact.

There's no question about it: Being exposed to cyber risk is an inevitable part of doing business in today's world. In fact, a recent [ESG study](#) found that 82% of organizations believe that cyber risk has increased over the past two years.

This finding isn't surprising. While the ongoing wave of digital transformation opens up exciting opportunities for innovation, it also expands your attack surface — exposing your organization to ever-evolving cyber risks. Maintaining continuous visibility into your critical assets is increasingly difficult. To make matters more complex, global cybercrime is on the rise. According to a [Cybersecurity Ventures](#) report, global cybercrime costs are expected to grow by 15% per year over the next five years — reaching \$10.5 trillion USD annually by 2025.

In many organizations, cyber risk is seen as complex and too often discussed with unfamiliar technical jargon or through the lens of incident remediation. According to the ESG study, 69% of business and technology leaders believe cybersecurity is entirely or mostly a technology area with little or no linkage to the business. Given these insights, it's clear that non-technical stakeholders struggle to understand how cyber risk translates into business risk.

Risk impacts a broad range of stakeholders — from the CRO to the CFO. Introducing a common language is critical to developing a comprehensive risk management strategy. To bridge the language gap between security and the business, cybersecurity leaders are turning towards analyzing cyber risk in the same way the organization looks at other issues: in terms of its financial impact. Understanding the financial impact of risks informs which ones to accept, mitigate, or transfer. Furthermore, it helps to identify the value of risk mitigation efforts.

With [BitSight Financial Quantification for Enterprise Cyber Risk](#), it's easier than ever to assess your financial exposure — and provide data-driven risk quantification insights that make sense to business stakeholders.

QUANTIFYING CYBER RISK USING PROVEN MODELS DEVELOPED FOR CYBER INSURANCE

**BitSight Financial
Quantification for Enterprise
Cyber Risk simulates your
organization's financial
exposure across multiple
types of cyber events
and impact scenarios
to calculate a range
of potential financial
losses. Armed with these
quantification insights, you
can make cybersecurity
investment decisions based
on what's best for the
business.**

Security leaders recognize the value of financial quantification. But traditional approaches lead to long, complex projects. These projects are complex because of the effort required to collect necessary data and the expertise needed to model various cyber risks to calculate a risk exposure range. This quantification process isn't easily repeatable.

With BitSight Financial Quantification, you can streamline the process of quantifying your cyber risk financially — without investing in any additional headcount or resources. The offering simulates your organization's financial exposure across multiple types of cyber events and impact scenarios to calculate a range of potential financial losses. Armed with these quantification insights, you can make cybersecurity investment decisions based on what's best for the business.

The world's largest insurance and reinsurance carriers use the underlying models — powered by [Kovrr](#) — that drive the BitSight Financial Quantification. This process involves assessing multiple types of losses (attritional losses, large losses, and catastrophe losses) as well as multiple types of events (specific events and systemic events). Leveraging these evolving cyber risk models enables underwriters and exposure managers to efficiently price risk. Today, this process is used to manage billions of dollars of cyber exposure.

BitSight Financial Quantification brings the same expertise to your security and risk management program. The solution combines technographic data, firmographic data, cyber insurance claims data, and cyber scenario probability calculations to quickly and easily simulate your organization's financial exposure across multiple types of business impact scenarios, including:

- **Denial of service incidents:** Events that are meant to shut down a machine or network, making it inaccessible to its intended users
- **Ransomware and extortion attacks:** Campaigns that infiltrate organizations by exploiting unpatched software vulnerabilities that can expose the organization to major data losses or extortion in exchange for the data returned
- **Data theft and privacy:** The act of stealing digital assets stored on computers, servers, or electronic devices with the intent to compromise privacy or obtain confidential information
- **Third-party service provider failures:** An outage, a degradation, or a disruption at the source causing the service provided to be temporarily unavailable or unreliable — or a malicious attack or event leading to data leakage, data alteration, or interruption of the service used
- **Regulatory compliance issues:** The failure to meet specific cybersecurity standards and regulations
- **Third-party liability:** Compensation claims against the organization when it's believed that the organization is responsible for a third party's damages or losses

Traditional financial quantification offerings only provide a high-level view of the overall magnitude of your exposure followed by data on a series of technical events. By bundling thousands of potential events into the above impact scenarios, the BitSight Financial Quantification takes your financial exposure insights further — empowering you to develop a common language through which your organization can discuss potential gaps in your security program and prioritize remediation efforts.

This approach models potential loss types independently — combining the results to deliver an analysis of probable maximum loss. Armed with these insights, you can establish a universal understanding of the business impact of cyber risk across your organization — and drive strategic conversations around which risks to accept, mitigate, or transfer.

Developing a mature program in today's evolving cybersecurity landscape requires a constant flow of high-quality, validated data that assesses how both your organization's security posture and the threat landscape are changing over time.

What types of data are incorporated into the quantification process?

Developing a mature program in today's evolving cybersecurity landscape requires a constant flow of high-quality, validated data that assesses how both your organization's security posture and the threat landscape are changing over time.

The BitSight Financial Quantification models automatically pull in three initial types of data inputs:

1. Company mapping

This company tree assessment is used to understand the structure of parent entities and subsidiaries. The BitSight platform automatically pulls in this data from its Ratings Tree.

2. Technographic data

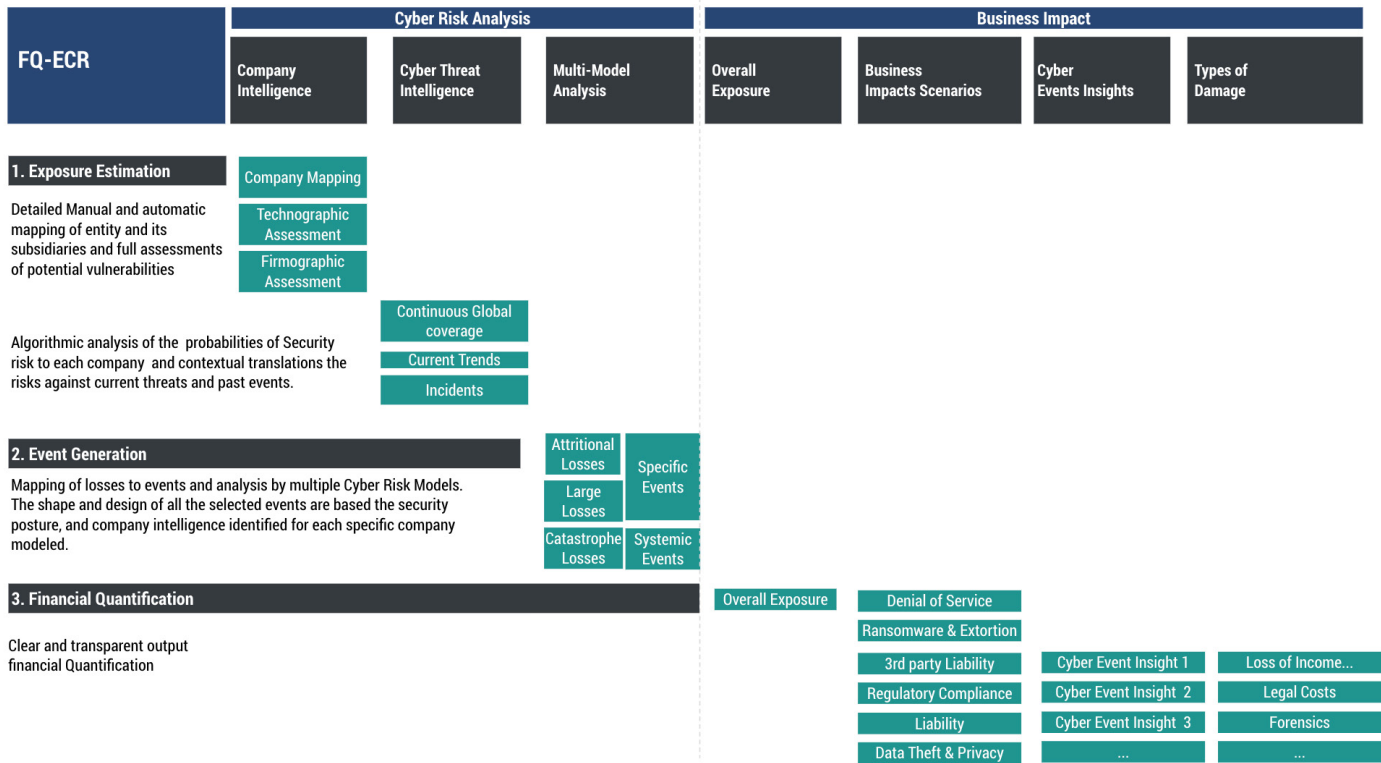
This category encompasses data collected around which technologies, services, and data centers each entity relies on. While digital asset data is used to understand the digital scale of a company (and, in doing so, estimate the potential magnitude and duration of a cyber attack), diligence data is used to understand the potential exposure of the company to different cyber events.

As organizations have an ever-evolving attack surface composed of a variety of different assets, gaining this context manually can be challenging. To streamline the process, the BitSight platform automatically pulls in relevant risk vector data that make up its security ratings, such as data around open ports, server configurations, insecure systems, patching cadence, and publicly disclosed security incidents.

3. Firmographic data

This category encompasses business information data used in conjunction with other types of data (such as cyber and non-cyber claims data) to inform the model's severity calculations. Some examples of data incorporated into the model here are revenue, number of employees, location of the business, industry type, number of customers, and number of sensitive data records maintained by the organization.

While the above sections outline the three data categories that are built into the model, organizations can also add data to assess their financial exposure. For example, additional data could reflect security controls, critical in-house technologies, and/or specific information of operational importance.



How does multi-model analysis work?

As cyber risk is not a monolithic problem, BitSight Financial Quantification leverages a three-stage, multi-model analysis:

1. Estimating exposure

The exposure estimation is based on BitSight’s data regarding the organization’s security posture — including technographic data around which service providers and technology the organization is using. This outside-in visibility into the organization’s attack surface empowers the model to understand the organization’s potential vulnerabilities and the degree of damage that could be caused by particular cyber event types.

The model pulls from tens of millions of data points of past cyber events (covering 130+ countries across 100+ different industries) and parameterizes the thousands of characteristics of each event based on the underlying distribution of technology exploitation patterns and past failure patterns of third-party service providers.

2. Creating a cyber event catalog

The purpose of this phase is to generate a comprehensive event catalog containing all possible events that can happen in the next year — which is essential to predicting financial damage. In order to do so, BitSight leverages Kovrr's proprietary modeling framework named "Impact Based Modeling." This framework models losses for the next year by focusing on the impact of cyber events. The model pulls from tens of millions of data points of past cyber events (covering 130+ countries across 100+ different industries) and parameterizes the thousands of characteristics of each event based on the underlying distribution of technology exploitation patterns and past failure patterns of third-party service providers. This includes specific downtimes and issues at the data center level. The model generates hundreds of thousands of synthetic events to create an event catalog that represents reality.

The size and structure of the event catalog are unique for each specific organization — based on that organization's security posture and company intelligence data. The actual events in the catalog are dependent on the latest BitSight data — and therefore can change. For instance, BitSight's compromised systems and public disclosures data are used to determine if an organization has experienced or is experiencing a security incident, while BitSight's diligence and user behavior data are used to model other cyber events that could potentially affect that organization.

3. Quantifying risk

In this step, the model determines the magnitude of damage an event will cause leveraging BitSight's data about assets and compromised systems. For instance, data on the importance of the organization's assets is used to understand the impact of a denial of services incident — assuming that the more important the asset is, the higher the financial damage will be.

After simulating an event, the model determines the financial impact on the business by comparing financial impact from similar events impacting companies with the same profile, industry, geography, and business size.

As BitSight Security Ratings are [proven to correlate to the likelihood of a breach](#), the BitSight Financial Quantification model uses this metric as a key KPI in its Monte Carlo simulation — an approach in which the following year is simulated 10,000 times in order to calculate a potential distribution of losses.

What types of business insights does this multi-model approach provide?

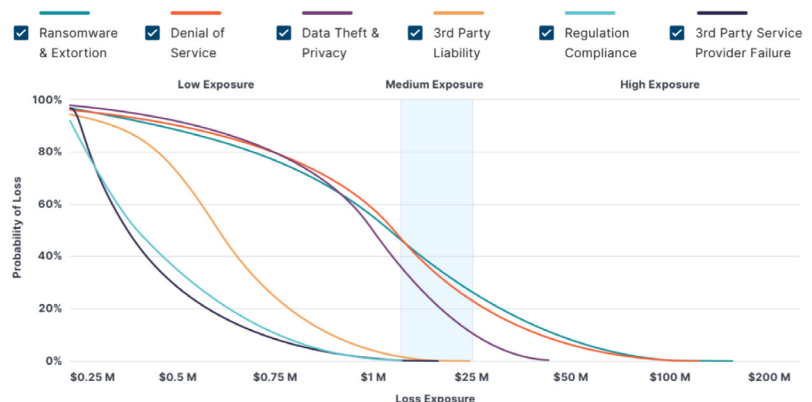
Overall, the model delivers a consistent and more representative view of your organization's cyber risk. Here, it's essential to differentiate between attacks and failures — and understand that both have the potential to cause financial (and reputational) damage. While an attack involves a malicious actor seeking to leak data, alter data, or interrupt the service, a failure involves an outage or disruption at the source (i.e., email provider, cloud provider, DNS provider) that causes the service provided to be temporarily unavailable or unreliable.

As both attacks and failures impact your business, insights into your corresponding financial exposure empower you to communicate cyber risk holistically across your organization so that you can make more informed decisions on budget allocation and risk transfer options.

As both of these types of events impact your business, insights into your corresponding financial exposure empower you to communicate cyber risk holistically across your organization so that you can make more informed decisions on budget allocation and risk transfer options.

The results of the modeling process are displayed in an exceedance probability (EP) graph, which shows the probability for suffering different financial losses from cyber events — broken down by impact scenario and overall magnitude of exposure. These calculations on the potential financial damage are produced based on an understanding of two factors: how it will affect the business (i.e., liability, business Interruption) and the parameters of the event in question (i.e., duration, intensity, what's affected).

Risk Scenario Financial Risk Breakdown



The BitSight Financial Quantification also provides cyber event insights — descriptive narratives of the types of cyber events that could potentially affect your organization. These narratives incorporate a range of specific events (those that a single company may suffer) and systemic events (those that affect multiple companies at the same time), providing customers with tangible examples of real events that could cause financial damage.

HOW THE BITSIGHT FINANCIAL QUANTIFICATION EMPOWERS YOU TO MATURE YOUR CYBERSECURITY PROGRAM

The BitSight Financial Quantification is available on-demand, is easily repeatable, and can be run without adding any headcount.

Here are three ways the BitSight Financial Quantification empowers you to establish a universal understanding of cyber risk across your organization — ultimately enabling you to develop a more mature cybersecurity program:

1. Streamline your process for quantifying cyber risk

Now more than ever before, it's critical to build a strategic [security performance management](#) program in which you take a risk-based, outcome-driven approach to measuring, monitoring, managing, and reporting on your organization's cybersecurity program performance over time. Of course, in order to do so, you need a framework to assess your exposure to cyber risk and lead meaningful conversations on its business impact.

Traditional financial quantification methods often rely on consulting engagements or long data collection processes — resources that most organizations are not willing or able to invest in on an ongoing basis. In contrast, the BitSight Financial Quantification is available on-demand, is easily repeatable, and can be run without adding any headcount. With the ability to drill down into cyber event examples — including damage types and other relevant data — security and risk management leaders can diagnose the underlying causes that impact financial exposure in a faster, more streamlined way than ever before.

And because this turnkey solution builds off of existing BitSight and Kovrr data, you can implement it quickly and easily — without investing in any additional resources.

With the BitSight Financial Quantification, you can use real-time data to inform decisions around which risks to accept, mitigate, or transfer – and where to focus your team's limited time, resources, and budget.

2. Make more informed business decisions

As the risk profile of an organization frequently changes, the ability to make data-driven decisions on where to focus your organization's cybersecurity efforts is more important than ever before. By prioritizing new technology investments based on risk reduction, you can optimize your program's ROI. Once you have assessed your current security posture and identified the gaps in your security program, you should be asking yourself the following types of questions:

- Which gaps would be the most impactful to remediate in terms of my organization's security posture?
- How much would the necessary controls cost? Can our organization afford it?

With the BitSight Financial Quantification, you can use real-time data to inform decisions around which risks to accept, mitigate, or transfer — and where to focus your team's limited time, resources, and budget.

BitSight's solution organizes loss exposure into specific business impact scenarios — highlighting any gaps in your security program. This added context enables you to view cyber risk through the lens of the potential business impact and facilitate resource prioritization and future planning with increased confidence.

3. Report to the board effectively

As cyber risk continues to increase, more and more boardroom conversations are focused on cybersecurity program performance. Business leaders want to learn more about the risks they face, but traditional scorecards or point-in-time snapshots are incomplete. These conditions make it challenging for stakeholders to connect cybersecurity data to real business risk.

As the BitSight Financial Quantification enables you to quantify your risk over time, it's easier than ever to demonstrate the impact and effectiveness of your efforts by measuring how your financial exposure changes as you invest in controls to improve your security posture.

With the BitSight Financial Quantification, you can transform the technical side of cybersecurity into financial language — aligning cyber risk conversations with how other types of risk are discussed and quantifying it like other initiatives that receive funding. By leveraging this framework to speak the same language as the board and provide the necessary business context, you can guide strategic conversations around managing your cyber risk, prioritizing new technology investments, and measuring the ROI of those investments in specific controls or programs. As the BitSight Financial Quantification enables you to quantify your risk over time, it's easier than ever to demonstrate the impact and effectiveness of your efforts by measuring how your financial exposure changes as you invest in controls to improve your security posture.

Ultimately, this greater understanding of cyber risk at the board level strengthens leadership's ability to deliver better and more secure business outcomes for your investors, business partners, and customers.

ELEVATE CYBER RISK TO BUSINESS RISK

In today's environment, cyber risk is increasing and of high concern to business leaders. But cyber risk is often thought about in technical terms as opposed to business terms — and more education on cyber risk is needed to increase cybersecurity engagement at the board level.

By quantifying cyber risk financially, you can establish a common language through which to assess the gaps in your security program and lead meaningful conversations on the business impact of different cyber scenarios and investments with the board. Ultimately, this empowers your organization to make more informed decisions about which risks to accept, mitigate, or transfer.

Interested in learning more about how the BitSight Financial Quantification makes it easier than ever to facilitate a greater understanding of cyber risk across your organization? Go to <https://www.bitsight.com/financial-quantification-for-enterprise-cyber-risk> or contact sales@bitsight.com.



111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Fifty percent of the world's cybersecurity premiums are underwritten by BitSight customers, and 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog or follow [@BitSight](https://twitter.com/BitSight) on Twitter.