+357 96 030922
info@marketpublishers.com

Cyber Risk Quantification Market Forecasts to 2032 – Global Analysis By Component (Platforms, Services, Consulting and Analytics Tools), Risk Type, Deployment, Organization Size, End User and By Geography

https://marketpublishers.com/r/C3AE8211329CEN.html
Date: November 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: C3AE8211329CEN

Abstracts

According to Stratistics MRC, the Global Cyber Risk Quantification Market is accounted for $0.37 billion in 2025 and is expected to reach $0.80 billion by 2032 growing at a CAGR of 11.3% during the forecast period. Cyber Risk Quantification is a disciplined process that evaluates cyber threats by estimating their potential financial losses through analytical models. Instead of relying on subjective ratings, it provides clear numerical values to represent the impact of security breaches. This approach helps organizations identify critical weaknesses, manage risk priorities, and distribute cybersecurity budgets more effectively. By converting technical issues into business-relevant insights, it improves communication with executives and supports regulatory compliance. Risk quantification also enables simulation of diverse attack scenarios, helping firms gauge probable outcomes and measure control performance. Ultimately, it empowers organizations to make informed decisions and align cybersecurity strategies with broader business objectives.

According to PwC's Global Digital Trust Insights 2025 survey, data reveals that only 15% of organizations are measuring cyber risk to a significant extent, highlighting a major gap in quantification practices despite rising board-level demand.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Rising frequency & sophistication of cyberattacks

Growing cyber threats, both in frequency and sophistication are driving rapid adoption of Cyber Risk Quantification solutions. Modern attacks—ransomware, multi-vector intrusions, supply-chain compromises, and AI-powered exploits—make it difficult for organizations to evaluate their true financial exposure using traditional qualitative methods. Expanding digital environments, including cloud platforms, hybrid workforces, and IoT ecosystems, further amplify uncertainties. Quantification platforms offer clear monetary estimates for data theft, downtime, system disruption, and extortion. As threat actors become more capable and targeted, organizations increasingly depend on detailed quantification models to prioritize controls, improve decision-making, and obtain executive approval for enhanced cybersecurity budgets.

Restraint:

Limited availability of high-quality data

A key barrier to Cyber Risk Quantification adoption is the scarcity of comprehensive, trustworthy data essential for producing dependable financial impact assessments. Many organizations lack detailed cyber incident histories, cost breakdowns, or standardized reporting practices, restricting effective model development. Complex IT setups, legacy systems, and siloed infrastructures create additional data inconsistencies that reduce quantification accuracy. Strict privacy and data protection rules also limit access to sensitive information needed for precise modeling. Without consistent, high-quality inputs, quantification platforms cannot confidently predict probabilities or financial losses. Consequently, companies may question the credibility of results and become reluctant to rely on quantification tools for strategic decisions.

Opportunity:

Expansion of AI-driven and automated risk modeling

AI-enabled and automated risk models present a major growth opportunity for the Cyber Risk Quantification Market. With increasing demand for faster, more reliable assessments, AI can process complex datasets, identify threat behaviors, and produce financial risk estimates with improved precision. Automation helps reduce reliance on scarce cybersecurity and analytics specialists, lowering overall operational burdens. Machine learning systems refine calculations continuously using updated threat feeds, ensuring consistent accuracy. This allows organizations to obtain real-time, adaptive

+357 96 030922
info@marketpublishers.com

risk metrics that strengthen proactive planning. As AI capabilities advance, quantification platforms will become more scalable, affordable, and widely adopted across industries.

Threat:

Rapidly evolving cyber threat landscape

One significant threat to the Cyber Risk Quantification Market is the speed at which cyber threats evolve, often surpassing the adaptability of existing quantification models. New attack types—AI-enabled breaches, deepfake manipulation, and multi-layered supply-chain intrusions—may not be accurately captured by outdated frameworks. As cybercriminals innovate rapidly, model accuracy can decline, causing organizations to lose confidence in financial risk estimates. Companies using static or infrequently updated models may miscalculate exposure, creating dangerous blind spots. This volatility pressures vendors to consistently upgrade tools, incorporate real-time threat intelligence, and build highly adaptive modeling systems to ensure ongoing reliability in dynamic threat environments.

Covid-19 Impact:

The Covid-19 pandemic created strong momentum for the Cyber Risk Quantification Market by accelerating digital dependence and exposing organizations to higher levels of cyber risk. With remote work expanding attack surfaces, incidents such as ransomware, credential theft, and cloud intrusions grew sharply, forcing companies to seek more accurate ways to measure financial exposure. Qualitative methods proved inadequate in the shifting threat landscape, leading executives to favor quantification for clearer decision-making under budget constraints. These tools helped businesses evaluate loss scenarios, prioritize controls, and demonstrate investment value. As a result, Covid-19 elevated quantification from optional support to a critical component of modern cybersecurity strategies.

The financial risk segment is expected to be the largest during the forecast period

The financial risk segment is expected to account for the largest market share during the forecast period because enterprises focus heavily on assessing the monetary consequences of cyber threats. Organizations require precise estimates of breach-related costs, ransomware impacts, operational downtime, and post-incident recovery to guide strategic spending. Quantification platforms translate technical exposures into

+357 96 030922
info@marketpublishers.com

financial insights, enabling leadership teams to make informed, budget-aligned decisions. As boards increasingly push for financial accountability in cybersecurity programs, businesses depend on models that forecast potential losses and compare risk levels with mitigation investments. This strong focus on economic clarity and measurable outcomes positions the financial risk segment as the dominant area within quantification efforts.

The cloud-based segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud-based segment is predicted to witness the highest growth rate as enterprises adopt cloud-first strategies and seek more adaptable security tools. Cloud-based quantification solutions deliver rapid setup, lower operational overhead, and better compatibility with modern cloud infrastructures. With businesses increasingly relying on multi-cloud ecosystems, they need platforms capable of evaluating risks across diverse, fast-changing environments. Cloud-enabled systems offer automated updates, scalable analytics, and continuous access to collective threat intelligence, enhancing accuracy and responsiveness. These advantages make cloud deployments more appealing than traditional setups, resulting in accelerated adoption and positioning the cloud-based segment as the fastest-growing area in this market.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by its advanced cybersecurity ecosystem, leading enterprises, and demanding regulatory environment. The United States is especially influential, backed by strong innovation in quantification technology, risk assessment, and insurance underwriting. Large organizations in this region prioritize translating risk into financial terms, which heightens demand for quantification platforms. The region’s deep threat intelligence capabilities, combined with significant investments in cyber risk modeling and board-level reporting, further bolster adoption. This strategic focus establishes North America as the benchmark for cyber risk quantification globally.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR. This surge is driven by rapid digital transformation in economies like China, India, and Japan, and the corresponding increase in cyber threat exposure. Enterprises in the region are rapidly deploying cloud-based and quantification-focused platforms to

+357 96 030922
info@marketpublishers.com

monitor and measure their risk in real time. Meanwhile, tighter cybersecurity regulations and national strategies on cyber resilience bolster demand even more. As organizations modernize and digitize, Asia-Pacific is poised to lead the market expansion for cyber risk quantification tools.

Key players in the market

Some of the key players in Cyber Risk Quantification Market include Bitsight Technologies Inc., SecurityScorecard Inc., RiskLens Inc., CyberCube Analytics Inc., Safe Security Inc., Balbix, Inc., Kovrr, Oliver Wyman Inc., PwC (PricewaterhouseCoopers), Protiviti Inc., IBM, Optiv Security Inc., ISACA, Axio Global and KPMG.

Key Developments:

In November 2025, IBM and Atruvia AG have sealed a long-term collaboration that paves the way for sustainable and state-of-the-art IT platforms for the banking of tomorrow. Atruvia will use IBM z17, which was announced earlier this year, as a cornerstone support its mission critical operations including the core banking system.

In September 2025, SecurityScorecard Inc. disclosed that it recently acquired HyperComply Inc., a Canadian startup that offers an artificial intelligence-powered platform for security questionnaire automation and compliance management, for an undisclosed sum. Founded in 2019, HyperComply offers a platform that helps both sales and security teams respond to security questionnaires. The system combines machine learning and AI-assisted drafting with human verification to ensure answers are accurate while reducing the work and time needed.

In November 2024, BitSight Technologies, Inc. announced an agreement to acquire the cyber threat intelligence firm Cybersixgill for $115 million. Bitsight, a more than decade-old security rating company, aims to use the real-time intelligence collected by the Tel Aviv-based data firm to mitigate customer supply chain threats. Cybersixgill, formed in 2014 and formerly called Sixgill, looks at data from the deep and clear web, including chat groups, as well as underground criminal forums markets where specialized software is needed.

Components Covered:

Platforms

+357 96 030922
info@marketpublishers.com

- Services
- Consulting
- Analytics Tools

Risk Types Covered:

- Financial Risk
- Operational Risk
- Reputational Risk
- Compliance Risk

Deployments Covered:

- On-Premises
- Cloud-Based
- Hybrid

Organization Sizes Covered:

- Small & Medium Enterprises (SMEs)
- Large Enterprises

End Users Covered:

- Banking, Financial Services & Insurance (BFSI)

+357 96 030922
info@marketpublishers.com

- Healthcare
- Telecommunications
- Enterprise IT & Digital Services
- Energy
- Manufacturing
- Government

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain
  - Rest of Europe
- Asia Pacific

+357 96 030922
info@marketpublishers.com

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

- Saudi Arabia
- UAE
- Qatar
- South Africa
- Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments

+357 96 030922
info@marketpublishers.com

- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

10 GLOBAL CYBER RISK QUANTIFICATION MARKET, BY GEOGRAPHY

11 KEY DEVELOPMENTS

+357 96 030922
info@marketpublishers.com

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cyber Risk Quantification Market Forecasts to 2032 – Global Analysis By Component (Platforms, Services, Consulting and Analytics Tools), Risk Type, Deployment, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/C3AE8211329CEN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/C3AE8211329CEN.html