Cybersecurity Insurance Market Assessment, By Component [Solution, Services], By Insurance Type [Standalone, Tailored], By Coverage Type [First-party, Liability Coverage], By Enterprise Size [SMEs, Large Enterprise], By End-user [Healthcare, BFSI, IT and Telecommunication, Manufacturing, Retail, Others], By Region, Opportunities and Forecast, 2018-2032F

Market Report | 2025-01-09 | 232 pages | Market Xcel - Markets and Data

AVAILABLE LICENSES:

- Single User License $4500.00
- Muti-User/Corporate Licence $5700.00
- Custom Research License $8200.00

Report description:

Global cybersecurity insurance market is projected to witness a CAGR of 17.95% during the forecast period 2025-2032, growing from USD 16.75 billion in 2024 to USD 62.75 billion in 2032.
The global cybersecurity insurance market is poised for robust growth on several interlinking factors. Rising awareness amongst the organizations over the frequency and sophistication of cyber-attacks reported that the ransomware attacks also increase have led them to focus on the potential financial consequences of such events, thus increasing the need to look at robust risk management strategies, which is reflected through their reliance on cybersecurity insurance as an integral part of the overall security posture of organizations. This increased awareness is further enhanced by the regulatory compliance requirement that makes companies adopt complete cybersecurity measures, thereby pushing up the demand for insurance products tailored to these needs.
In addition, the digital transformation that is gaining momentum across all industries further enlarges the scope of the attack surface associated with cyber threats, and a stronger shield is required. Therefore, it is also calling for an increasing demand for special insurance for SMEs under the threat of cyber criminal activities against them. The use of artificial intelligence during the risk-assessing process further enhances the prospects of the effectiveness and appeal of cybersecurity insurance offerings. Strategic cooperation between cybersecurity companies and insurance companies also improves service provision and product innovation. All these factors are expected to create significant growth in the market for cybersecurity insurance.
For instance, in January 2024, as per the UK government, it was published that AI is already being used in malicious cyber activity

and will almost certainly increase the volume and impact of cyber-attacks, including ransomware in the near term. The report, among other conclusions, suggests that by lowering the barrier of entry to novice cybercriminals, hackers-for-hire, and hacktivists, AI enables relatively unskilled threat actors to carry out more effective access and information-gathering operations. This will lead to more use of cybersecurity insurance.

Rising Data Breaches and Ransomware Attacks Fuelling Market Growth

The most significant growth driver in the cybersecurity insurance market is rising data breaches and ransomware attacks. Organizations worldwide are witnessing more frequent cyber threats, which increases the demand for broad insurance coverage to minimize financial damage. Ransomware attacks involving malicious software that encrypts data until a ransom is paid are now one of the biggest risk factors. The ransomware tactics have evolved to become more sophisticated and have even led to the emergence of Ransomware-as-a-Service (RaaS), making these attacks more common and destructive. Moreover, data breaches, where sensitive information is accessed and stolen, have become more frequent and severe, causing organizations to incur significant costs related to notification expenses, data recovery, and legal fines.

The increased threat of ransomware and data breaches has brought greater awareness of cyber risks and has fuelled demand for robust insurance policies offering complete protection. With companies wanting to protect their digital assets and be in regulatory compliance, the cybersecurity insurance market will likely maintain an upward trend as a critical need for financial protection against these increasingly aggressive threats.

For example, in December 2024, US healthcare giant Ascension said a ransomware attack affected nearly six million customers. Hackers who struck Ascension with ransomware managed to steal a treasure trove of sensitive customer information, including medical information, personally identifiable information, payment data, and more. The US healthcare giant has now released new details about the ransomware attack and filed a new form with the Office of the Maine Attorney General.

Growing Demand for Crypto Insurance Services

The growing demand for crypto insurance services is the major driver of the growth of the cybersecurity insurance market. The increasing ownership of cryptocurrency around the world is increasing the related threats. High-profile incidents highlight vulnerabilities in the crypto space, which leads to huge financial losses for investors and a decline in market confidence. Companies are responding to these rising threats by investing in insurance policies that can counter crypto-related threats. This is further increasing the demand for more comprehensive cybersecurity insurance solutions.

The number of claims with cyber incidents has exposed a highly volatile risk environment, bringing about incessant premium raises for the policyholders. Of the emerging trends, AI exposures, concerns over data collection, risks of BEC, and ransomware threats are taking on critical meanings in the modern scheme of cyber insurance. In unison, these factors are reflective of the growing demand for heavy insurance coverage in the crypto sector and add much momentum to the expansion of cybersecurity insurance as an industry in general.

For example, in August 2024, Lloyd's of London has partnered with Evertas and Nayms to allow insurance policies for digital assets to be paid using cryptocurrency on the Ethereum blockchain. This marks a significant advancement in the insurance industry, making it easier for crypto holders to obtain coverage and pay premiums directly in digital currency. Previously, getting crypto insurance was challenging, but this collaboration highlights the progress made in offering tailored solutions for the growing crypto market.

Government Compliances Acting as a Catalyst

Government compliance is an essential driver for the growth of the global cybersecurity insurance market. Data protection regulations in the form of GDPR in Europe and CCPA in the United States are making it compulsory for organizations to protect personal data and report any breach. This regulatory environment makes cybersecurity insurance necessary for compliance, pushing businesses to invest in such policies to mitigate potential liabilities. Another is that efforts by governments to be aware of cybersecurity threats have helped organizations be aware of the value of their cybersecurity insurance.

In addition, it can lead to significant monetary fines if the organization is not in compliance with them. Cybersecurity insurance then becomes a critical tool to help organizations manage the monetary impacts of data breaches as well as regulatory fines imposed by governments. As these governments continue to strengthen the regulatory frameworks and impose stricter regulations on businesses, the need for cybersecurity insurance will likely increase.

For example, in August 2024, Kanematsu Corporation, Kanematsu Electronics Ltd., and Global Security Experts Inc. decided to

establish the "Nippon Cyber Security Fund 1 Investment Limited Partnership", the first fund in Japan to specially invest in security companies, with WERU Investment Co., Ltd. as its general partner. Against the backdrop of the spread of DX and the increasing sophistication of cyber-attacks, all companies and organizations in Japan are urged to respond to and take countermeasures against such attacks. As the number of companies and organizations targeted by attacks increases each year, and the scope and content of countermeasures continue to change, it is essential for security companies to join forces to face the challenges to protect Japanese companies from these threats.

Dominance of First-party Coverage Cybersecurity Insurances

First-party cyber insurance covers are now widely preferred due to their wide-ranging protection against direct loss arising from a cyber-related incident. Such coverage entails direct financial assistance for these various expenses, including, for example, response costs when there is a data breach, forensic investigation, business interruption losses, and managing the reputational damage by making public relations efforts to restore the corporate image after an attack. In addition, first-party coverage usually encompasses many kinds of expenses, such as costs for data recovery, expenses of notifications to affected customers, credit monitoring services, and even payments for cyber extortion.

First-party coverage can be attractive because of customization options to allow the organization to determine coverage limits. It can provide immediate financial help to support organizations to rebound quickly after a cyber event, hence minimizing downtime and operational disruptions.

For instance, in February 2024, Coalition announced enhancements to its cyber insurance policies, which now include comprehensive first-party coverage for businesses facing ransomware attacks and data breaches. Their policies cover expenses such as incident response, forensic investigations, and business interruption losses directly incurred by the insured due to cyber incidents. This move reflects the growing recognition of the need for robust first-party coverage in response to the increasing frequency and severity of cyber threats organizations face today.

North America Dominates Cybersecurity Insurance Market Share

North America leads the pack in the global market for cybersecurity insurance. Several interrelated factors contribute to this fact. The economy of the region is highly digitalized with massive technology adoption in almost all areas, so it becomes an easy and lucrative target for cyber hackers. This means that in the year 2023, in North America, over 900,000 cyber incidents were recorded. This shows that cybercrime has exponentially increased demand for cybersecurity insurance from businesses wanting to protect against financial loss.

Moreover, stringent regulatory compliance requirements, such as the California Consumer Privacy Act and federal initiatives to enhance cybersecurity frameworks, force organizations to adopt insurance policies to manage liabilities effectively. There is also growing awareness among businesses regarding the risks associated with cyber threats, leading to increased investment in cybersecurity measures. This is a scenario with high digitalization, regular cyberattacks, and increased regulatory pressures and awareness levels. It positions North America as a prime center for expansion in the cybersecurity insurance market, with growth prospects to remain very robust over the next couple of years.

For instance, in October 2024, The Travelers Indemnity Company, headquartered in New York, North America Reported Excellent Third Quarter and Year-to-Date Results. Fairfax Financial Holdings Limited, another company located in North America, reported higher profits as compared to 2023. This shows how cybersecurity insurance market is growing rapidly in North America.

Future Market Scenario (2025 – 2032F)

- Virtual agents will fundamentally revolutionize the assessment of risk through exposure quantification and by offering recommendations for cybersecurity. Risks will thus be much better and more proactive.
- Optimized active risk-based coverage creation ensures better, more tailored, and effective approaches to cybersecurity solutions and satisfies specific needs and vulnerabilities present in an organization.
- Advances in technology will enable faster and more effective incident monitoring and response, with streamlined claims processing, all helping minimize the impact of cyber incidents on businesses.
- Increased campaigns and efforts to raise awareness about cybersecurity and risk management solutions will strengthen overall resilience as organizations increasingly embrace robust security measures to protect against evolving cyber threats.

Key Players Landscape and Outlook

Continuous innovation characterizes the landscape of cybersecurity insurance globally, as the companies compete to outperform

one another in terms of GPU performance, energy efficiency, and unique features. The market prognosis remains positive, owing to increased demand for high-quality gaming, AI, and professional workloads. Cybersecurity Insurance manufacturers are concerned with supply chain resilience, energy efficiency, and environmental practices, which will likely define the industry's future. Collaborations and developing technologies are projected to increase competition in this fast-paced market.
In November 2024, Aon PLC launched its Cyber Risk Analyzer, a digital application that allows risk managers to make data-driven, technology-enabled decisions to mitigate cyber risk. The tool is the latest in a series of new offerings, which brings together Aon's data, tools, and analytics professionals to support clients through an evolving risk landscape across sectors. Aon's Cyber Risk Analyzer allows Aon's clients and brokers unique access to loss forecasting, exposure assessment, total cost of Risk (tcor) analysis and more.
In September 2024, Lloyd□s of London Limited opened a new office in Miami to strengthen its Latin America and Caribbean business and continue to support the market□s sustainable and profitable growth in the Americas. The new office will enable Lloyd□s to realign its resources to centrally support brokers, cover holders and managing agents throughout Spanish-speaking Latin America and the Caribbean, while creating another hub in the Americas to service overall business.

Table of Contents:

Cybersecurity Insurance Market Assessment, By Component [Solution, Services], By Insurance Type [Standalone, Tailored], By Coverage Type [First-party, Liability Coverage], By Enterprise Size [SMEs, Large Enterprise], By End-user [Healthcare, BFSI, IT and Telecommunication, Manufacturing, Retail, Others], By Region, Opportunities and Forecast, 2018-2032F

Market Report | 2025-01-09 | 232 pages | Market Xcel - Markets and Data

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4500.00
	Muti-User/Corporate Licence	$5700.00
	Custom Research License	$8200.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	

Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature	