

# Opportunities and Challenges in the Global Cyber Insurance Market

July 2021: Complimentary Abstract / Table of Contents



# Our research offerings

This report is included in the following research program(s):

## Insurance ITS

- ▶ Application Services
- ▶ Banking & Financial Services BPS
- ▶ Banking & Financial Services ITS
- ▶ Catalyst™
- ▶ Clinical Development Technology
- ▶ Cloud & Infrastructure
- ▶ Conversational AI
- ▶ Contingent Workforce Management
- ▶ Cost Excellence
- ▶ Customer Experience Management Services
- ▶ Cybersecurity
- ▶ Data & Analytics
- ▶ Digital Adoption Platforms (DAP)
- ▶ Digital Services
- ▶ Engineering Services
- ▶ Enterprise Platform Services
- ▶ Finance & Accounting
- ▶ Financial Services Technology (FinTech)
- ▶ Global Business Services
- ▶ Healthcare BPS
- ▶ Healthcare ITS
- ▶ Human Resources
- ▶ Insurance BPS
- ▶ Insurance ITS
- ▶ Insurance Technology (InsurTech)
- ▶ Insurance Third-Party Administration (TPA) Services
- ▶ Intelligent Document Processing (IDP)
- ▶ Interactive Experience (IX) Services
- ▶ IT Services Executive Insights™
- ▶ Life Sciences BPS
- ▶ Life Sciences ITS
- ▶ Locations Insider™
- ▶ Market Vista™
- ▶ Mortgage Operations
- ▶ Multi-country Payroll
- ▶ Network Services & 5G
- ▶ Outsourcing Excellence
- ▶ Pricing-as-a-Service
- ▶ Process Mining
- ▶ Procurement
- ▶ Recruitment Process Outsourcing
- ▶ Rewards & Recognition
- ▶ Service Optimization Technologies
- ▶ Supply Chain Management (SCM) Services
- ▶ Talent Excellence GBS
- ▶ Talent Excellence ITS
- ▶ Workplace Services
- ▶ Work at Home Agent (WAHA) Customer Experience Management (CXM)

If you want to learn whether your organization has a membership agreement or request information on pricing and membership options, please contact us at [info@everestgrp.com](mailto:info@everestgrp.com)

Learn more about our  
**custom research capabilities**

Benchmarking

Contract assessment

Peer analysis

Market intelligence

Tracking: service providers, locations, risk, technologies

Locations: costs, skills, sustainability, portfolios

# Contents

For more information on this and other research published by Everest Group, please contact us:

**Ronak Doshi**, Vice President

**Aaditya Jain**, Practice Director

**Supratim Nandi**, Practice Director

**Keerthi Vuchula**, Senior Analyst

**Mehul Khera**, Senior Analyst

**Shrey Kalawatia**, Senior Analyst

**Vigitesh Tewary**, Senior Analyst

**Satwik Tripathi**, Analyst

<b>1. Introduction and overview</b>	<b>5</b>
• Research methodology	6
• Background and/or introduction	7
• Executive summary	8
<b>2. Cyber Insurance market dynamics</b>	<b>9</b>
• Cyber insurance market dynamics	10
• Key drivers of cyber insurance	11
• Regional view of cyber insurance	12
<b>3. Challenges faced by cyber insurers and enterprises</b>	<b>13</b>
• Challenges faced by cyber insurers	14
• Challenges faced by enterprises	16
<b>4. Spotlight:</b>	<b>17</b>
• Threat from cloud	18
<b>5. Initiatives by cyber insurers and enterprises to address industry challenges</b>	<b>19</b>
• Initiatives taken by cyber insurers	20
• Initiatives taken by enterprises	21
<b>6. Regulatory updates</b>	<b>22</b>
• Regional regulatory updates around cybersecurity and cyber insurance	23

# Contents

<b>7. Cyber and IT security vendor landscape</b>	<b>24</b>
• IT security service provider vendor landscape	25
• Cybersecurity and cyber data vendor landscape	26
<b>8. Strategic implications for service providers and the future of cyber insurance</b>	<b>27</b>
• Strategic implications for enterprises	28
• Strategic implications for IT service providers	29
• Future of cyber insurance	30
<b>9. Appendix</b>	<b>31</b>
• Glossary	32
• Research calendar	33

# Our research methodology is based on four pillars of strength to produce actionable and insightful research for the industry

01

### Robust definitions and frameworks

Line of Business (LoB) and value chain-specific coverage, SUPER experience framework, and insurer of the future framework

02

### Primary sources of information

Annual contractual and operational RFIs, service provider briefings and buyer interviews, web-based surveys

03

### Diverse set of market touchpoints

Ongoing interactions across key stakeholders, input from a mix of perspectives and interests, supports both data analysis and thought leadership

04

### Fact-based research

Data-driven analysis with expert perspectives, trend-analysis across market adoption, contracting, and service providers

Proprietary contractual database of over 500 insurance IT services contracts (updated annually)

Year-round tracking of 25+ insurance IT service providers

Large repository of existing research in insurance IT services

Over 30 years of experience advising clients on strategic IT, business services, engineering services, and sourcing

Executive-level relationships with buyers, service providers, technology providers, and industry associations

## Background of the research

### Background of the research

The intensity and severity of cyber events has accelerated during the COVID-19 pandemic as more and more people are working remotely and from home. This increasing frequency of cyberattacks has brought volatility to the already spiking claims losses causing many to wonder how enterprises and insurers can manage cyber risks in this new era. The pandemic has forced enterprises to rapidly shift to a remote/work-from-home format, compelling them to rethink their cybersecurity strategies, reassess their cyber threat exposures, and develop cyber policy plans that can adequately manage any potential threats. Enterprises are not alone. Insurers have been significantly impacted by the rapid growth of cyber-attacks and burdened with the dramatic increase in claims losses from the policies sold.

To address these challenges enterprises and insurers alike are making investments in technologies such as network security, identity access management, cyber security analytics, AI/ML, and real time threat detection, among others. While enterprises are beefing their cybersecurity capabilities and investing in the right set of technology and talent levers to bolster cyber risk assessment capabilities, insurers are identifying the full set of dependencies to assess the complete severity of attack.

In this report we focus on the current state of the cyber insurance market and discuss the different challenges faced by insurers and enterprises as well as how they plan on addressing them. We also capture the technology vendor landscape that can support enterprises and insurers in their journey for cybersecurity and cyber insurance.

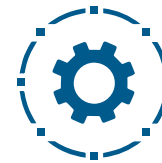
### Scope of this report:



**Geography**  
Global



**Industry**  
Cyber insurance



**Services**  
Cybersecurity services

## Executive summary



### Cyber insurance market landscape

- The global cyber insurance market has been growing by more than **20%** over the last three years and is expected to continue this trajectory over 2020-23
- This growth will be led by **Europe and Asia Pacific** due to the increasing frequency and severity of attacks and the growing awareness and need of cyber policies within the SME segment



### Challenges faced by enterprises and cyber insurers

- **Lack of historical data** and the inability to accurately price cyber risks remains a key challenge for insurers; this has led to **increasing loss ratios** and declining profitability
- Enterprises, on the other hand, are struggling with **deploying a reliable cyber resilience plan** and need support from managed security service providers and cybersecurity firms to shield it from cybercrime



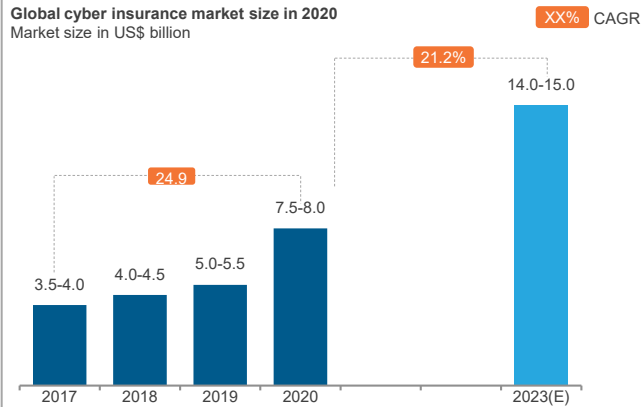
### Implications and future of cyber insurance

- Service providers are investing in enhancing their **consulting/advisory offerings around cyber risk analytics** to help enterprises assess their cyber risk exposure and develop an adequate cybersecurity response plans
- Going forward, enterprises, managed service providers, and cybersecurity firms are expected to work in tandem in an **ecosystem** while leveraging each other's capabilities

# This study offers eight distinct chapters providing a deep dive into key aspects of cyber insurance market; below are four charts to illustrate the depth of the report

## Cyber insurance market dynamics

**Global cyber insurance market size in 2020**  
Market size in US\$ billion



- The global cyber insurance premiums increased by nearly 50% YoY to reach US\$7.5-US\$8 billion in 2020, due to increasing cyber risks on account of the sudden shift from a physical to remote working environment
- This growth was also supported by 5%-10% increase in the premium rates on account of increasing losses for insurers from frequent and severe cyberattacks; in 2020, the global average cost of a data breach reached US\$3.86 million, from US\$3.62 million in 2017
- Due to the increasing cost of cyberattacks, insurers have been struggling with declining profitability on account of increasing loss ratios
- The key cost driver for claims has been business interruption losses due to the high cost of system downtime, restoration, and incidence response
- Another such trend in the cyber insurance market is the imposition of coverage restrictions for riskier industries, such as healthcare and education, due to the high cost of data breaches and other cyber threats
- Enterprises, globally, are deploying cybersecurity solutions that comprise technologies, such as IAM and network security, among others; they are also implementing a comprehensive cyber risk response plan along with investing in bundled cyber insurance

## Key challenges faced by cyber insurers

### Challenges faced by cyber insurers

#### Limited historical data on cyber losses and events

- Limited availability of historical loss and cyber event data curtails the development of cyber loss modeling to quantify the risk; as a result, insurers face challenges in accurately underwriting cyber risk
- One of the causes for lack of data is that relatively fewer cyber events are reported as compared to the actual attacks

#### Increasing loss ratios putting pressure on insurer profitability

- Loss ratio for the global cyber insurance market is increasing owing to the increasing frequency and severity of attacks including data breaches, ransomware attacks, among others
- Growing loss ratios are expected to eat into the insurer profitability for the cyber security segment; insurers will have to act in this area to control the growing losses

#### Evolving nature of cyber attacks

- With new emerging technologies, the nature of cyber risk is also continuously evolving, thus limiting the insurer's ability to accurately evaluate the cyber risk
- For instance, while the introduction of quantum computing is revolutionizing the field of analytics, it is also impairing the existing encryption systems in place

1. US Department of Homeland Security
2. Fitch Ratings
3. Munich Re



#### 7-10 years

Insurance companies have typically 7 to 10 years of cyber insurance claims data to support underwriting and modeling<sup>1</sup>



#### 73%

The direct loss ratio for stand-alone cyber insurance increased in 2020 to 73%, rising from 49% in 2019; the highest ever since 2015<sup>2</sup>



#### US\$17 billion

Sophisticated ransomware attacks led to US\$17 billion worth of economic losses; in 2021, the same have been recorded at US\$20 billion (till date)<sup>3</sup>

## Key initiatives from cyber insurers

NOT EXHAUSTIVE					
<b>Endpoint protection</b> Insurers are partnering with endpoint protection cyber security firms to offer a combined solution of cyber insurance and threat monitoring	<b>Identity theft</b> Insurers are collaborating with the identity management firms to address the concern of loss of personal data by the customers in addition to a cyber insurance offering	<b>Compliance</b> Insurers are partnering with compliance firms to help customers reduce time to obtain compliance and reduce the risk of fines	<b>Cyber analytics</b> Insurers are investing in cyber analytics to develop accurate pricing models, and reinforce accumulation risk management	<b>Cyber threat assessment</b> Insurers are teaming up with cybersecurity rating providers or cyber risk scoring firms to better understand the SME's risk exposure	<b>Cloud security</b> Insurers are investing in cloud security to address the cloud risk, which has observed an uptick due to the increase in cloud adoption

### Key initiatives by cyber insurers

Coalition, a cyber insurance and security company, partnered with SentinelOne, an automated endpoint detection and response provider, to offer a bundled solution of cyber insurance and endpoint detection and response to its clients	Ray Sigorta, subsidiary of Vienna insurance group, has partnered with CPP Group to increase the scope of its cyber insurance product, which provides cover against both virtual and real identity theft by introducing online security checks within the product	Zeguro, a cybersecurity and cyber insurance provider, partnered with Vanta, an automated security and compliance provider, to help customers reduce time to achieve compliance from months to weeks	Hiscox, a US-based insurance company, is implementing CyberCube's cyber analytics technology to obtain insights to enhance its underwriting capabilities	Liberty Mutual, a global insurance provider, partnered with Security Scorecard, a cybersecurity rating provider, to get an analysis of the client's cybersecurity and the external threats they are exposed to	Google Cloud partnered with Allianz and Munich Re for a risk protection program that comes in two parts, i.e., first is a diagnostic tool to measure and manage Google Cloud customer's risk, and second is an insurance product
---	--	---	--	--	--

## Future of cyber insurance

Ecosystem of cyber insurance	Future of cyber insurance
<b>Cyber risk database</b> Partner with insurers to offer cyber risk databases, develop risk scoring frameworks, partner with enterprises to assess cyber risks	<ul style="list-style-type: none"> <li>• <b>Work from home security:</b> enterprises are likely to continue investing in network security and identity and access management tools that enable employees to work securely on any given network</li> <li>• <b>Cloud security:</b> with increasing cloud adoption, cloud-based security services will become a hot topic for enterprises to curb growing cyber-attacks</li> <li>• <b>Blurring lines between personal and commercial cyber insurance:</b> the remote working format is not likely to change in the near term, so insurers will offer enterprises personal cyber risk covers to shield consumers from any cyber-related risks</li> <li>• <b>Capping lines of coverage:</b> given the need for a sustainable policy that will not pose an imminent threat on the industry profitability, carriers are likely to cap the lines of coverage and increase rates while also diversifying current cyber risk portfolios</li> <li>• <b>Building a cyber insurance ecosystem:</b> carriers are expected to build a cyber insurance ecosystem to successfully underwrite cyber risk and consequently bring significant value to the enterprises, while also enhancing underwriting capabilities by leveraging real-time threat intelligence                             <ul style="list-style-type: none"> <li>– This will provide insurers with new data sources and insights to drive better risk evaluation and, in turn, build a more resilient cybersecurity landscape</li> </ul> </li> <li>• <b>Regulatory intervention:</b> industry regulators will also play a key role in risk underwriting with the introduction of regional cyber insurance risk frameworks as best practices for managing cyber risk</li> </ul>
<b>Insurers</b> Standardize cyber insurance offering, capping cyber coverage, increase rates, diversify portfolio, provide VAS	
<b>Cyber risk analytics</b> Partner with insurers to offer cyber risk databases, develop risk scoring frameworks, partner with enterprises to assess cyber risks	
<b>Cyber security providers</b> Provide IAM, network security, cloud security and API security to enterprises; partner with Insurers to offer VAS	
<b>IT service providers</b> Offer real time threat intelligence, develop cyber risk analytics capabilities, IT security managed services	

Source: Everest Group cyber insurance blogs



# Research calendar

## Insurance IT Services

■ Published
 ■ Planned
 ■ Current release

### Flagship Insurance IT Services reports

#### Release date

Insurance Business Model Innovation Enablement Services PEAK Matrix® Assessment 2020	November 2020
Insurance Business Model Innovation Enablement Services – Service Provider Compendium 2020	December 2020
Application and Digital Services (ADS) in Life and Annuities (L&A) Insurance – PEAK Matrix® Assessment 2021	December 2020
Application and Digital Services (ADS) in Life and Annuities (L&A) Insurance – Service Provider Compendium 2021	January 2021
Insurance IT Services – State of the Market 2021: Future-readying insurance business through continuous digital unraveling	January 2021
Insurance platform services PEAK Matrix assessment 2021	Q3 2021
Insurance platform services – Service provider profile compendium	Q3 2021
Digital experience platforms in Insurance – Product PEAK Matrix assessment 2021	Q3 2021
Application and digital services in P&C insurance – Services PEAK Matrix assessment	Q4 2021
Digital claims solutions PEAK Matrix assessment 2021	Q4 2021

### Thematic Insurance IT Services reports

#### Release date

Life & Annuities (L&A) Insurance Core Platform Software Adoption Trends – Unlocking Efficiency and Growth for L&A Insurers	December 2020
Cloud as a change catalyst in Insurance	May 2021
Digital Transformation in the London Insurance Market	July 2021
<b>Opportunities and Challenges in the Global Cyber Insurance Market</b>	<b>July 2021</b>
Policy administration platforms in the L&A insurance industry – Market report	Q3 2021
Digital experience solutions in the retirements industry – Market report	Q4 2021

Note: For a list of all of our published ITS | Insurance reports, please refer to our [website page](#)



Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our clients include leading global companies, service providers, and investors. Clients use our services to guide their journeys to achieve heightened operational and financial performance, accelerated value delivery, and high-impact business outcomes. Details and in-depth content are available at [www.everestgrp.com](http://www.everestgrp.com).

## Stay connected

### Website

[everestgrp.com](http://everestgrp.com)

### Social Media

-  @EverestGroup
-  @Everest Group
-  @Everest Group
-  @Everest Group

### Blog

[everestgrp.com/blog](http://everestgrp.com/blog)

### Dallas (Headquarters)

[info@everestgrp.com](mailto:info@everestgrp.com)  
+1-214-451-3000

### Bangalore

[india@everestgrp.com](mailto:india@everestgrp.com)  
+91-80-61463500

### Delhi

[india@everestgrp.com](mailto:india@everestgrp.com)  
+91-124-496-1000

### London

[unitedkingdom@everestgrp.com](mailto:unitedkingdom@everestgrp.com)  
+44-207-129-1318

### Toronto

[canada@everestgrp.com](mailto:canada@everestgrp.com)  
+1-647-557-3475

*This document is for informational purposes only, and it is being provided "as is" and "as available" without any warranty of any kind, including any warranties of completeness, adequacy, or fitness for a particular purpose. Everest Group is not a legal or investment adviser; the contents of this document should not be construed as legal, tax, or investment advice. This document should not be used as a substitute for consultation with professional advisors, and Everest Group disclaims liability for any actions or decisions not to act that are taken as a result of any material in this publication.*