

## **Cybersecurity Insurance Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)**

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

### **AVAILABLE LICENSES:**

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

### **Report description:**

The cybersecurity insurance market is registering a CAGR of 19.47% during the forecast period. Increasing digitalization and rapid development in the cloud, Big Data, IoT, and artificial intelligence (AI) in business and society and the growing connectivity of everything have increased the workload of already strained IT teams.

#### Key Highlights

IT advances, communication technologies, and the smart energy grid are changing the landscape of all every country's critical infrastructure and business networks. However, with rapidly evolving technology comes rapidly advancing threats. Personal data is valuable, which prompts cybercriminals to commit crimes, where personal information will be sold on the dark web, like a credit card number, identity, medical records, etc. It is among the few factors that have led to an increased demand for cybersecurity. Cloud computing is one of the most rapidly growing recent technologies, eliminating the traditional boundaries of IT, creating new markets, spurring the mobility trend, and enabling advances in unified communications. Various tech stakeholders and organizations are turning to new insurance models to mitigate the risks of storing sensitive data in the modern cybersecurity landscape.

As the cybersecurity insurance space continues to mature, insurers will consider a broader range of security controls and technologies in their assessments. Hence, the sensitivity level of an organization's data and its ability to adequately obscure it will play a key role in determining the overall risk, which is driving the adoption of new technologies like micro shading. Microsharding technology breaks data into fragments that can be as small as single-digit bytes before polluting and distributing shards to multiple locations to reduce the attack surface and eliminate data sensitivity.

Cyber insurance policies and businesses cover a wide range of risks, and insurers do not always agree on which loss events are covered. Cyber events have characteristics that make it challenging to write comprehensive policies, such as limited loss history, the unreliability of past data when predicting future events, and the possibility of a large-scale attack with highly correlated losses

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scottss-international.com](mailto:support@scottss-international.com)

[www.scottss-international.com](http://www.scottss-international.com)

across companies and industries. Furthermore, insurers are still working on precise and accurate criteria for cyberattacks and the impact of new technologies like the Internet of Things. Cyber insurance coverage could be ineffective and expose firms to considerable damage if big cyberattacks occur without well-defined dangers and an understanding of how they affect insurers. The pandemic accelerated the adoption of digital tools, which has driven a greater need for cybersecurity insurance coverage. Various companies have been looking forward to combining insurance with cybersecurity tools to help businesses mitigate and manage cyber risk. In 2020, Coalition, a cyber insurance company, acquired BinaryEdge, a platform akin to BitSight and Security Scorecard that searches the internet and maps an organization's attack surface. The Coalition has merged terabytes of data from BinaryEdge with claims and other cybersecurity data sources to enable its risk evaluation process with machine learning and natural language processing. Further, due to the ongoing COVID-19 pandemic, countries worldwide have implemented preventive measures. With schools being closed and communities being asked to stay at home, multiple organizations found a way to enable employees to work from their homes. This resulted in a rise in the adoption of video communication platforms. In the past 6-8 months, the new domain registration on these video communication platforms, including Zoom, rapidly increased.

## Cybersecurity Insurance Market Trends

### The BFSI Segment is Estimated to Hold a Significant Revenue Share of the Market Studied

The BFSI industry is one of the critical infrastructure segments facing multiple data breaches and cyberattacks, owing to the massive client base that the sector serves and the financial information at stake. Cybercriminals are optimizing myriad diabolical cyberattacks to immobilize the financial industry since it is a highly lucrative operating model with amazing profits and the bonus of relatively little risk and detectability. Trojans, ATMs, ransomware, mobile banking, data breaches, institutional invasion, data thefts, fiscal breaches, and other threats are all part of the threat environment for these attacks.

Cybersecurity Insurance is increasingly becoming a vital part of banking and financial institutions. The industry is expected to command a significant global market share during the forecast period. It is one of the highly regulated, governed industries and is also prone to identity frauds that augment demand.

For instance, in October 2021, the Federal Trade Commission issued an amended rule that increases the data security precautions financial institutions must implement to secure their clients' financial data. In recent years, consumers have suffered enormous suffering due to massive data breaches and cyberattacks, including monetary loss, identity theft, and other forms of financial misery. The revised Safeguards Rule from the Federal Trade Commission requires non-banking financial firms, such as mortgage brokers, car dealers, and payday lenders, to establish, implement, and maintain a robust security system to protect their clients' information. Government policies will significantly drive the market.

With increased security breaches, banks and financial institutes should adopt cybersecurity insurance to safeguard their customers' data and prevent economic losses. For instance, in December 2021, a huge security breach at Bitmart, a crypto trading platform, resulted in hackers removing about USD 200 million in assets. A stolen private key was the primary source of the security compromise, which affected two of its Ethereum and Binance innovative chain hot wallets.

Furthermore, in October 2021, SharkBot, a new Android banking Trojan, was uncovered by Cleafy and Threat Fabric researchers. The virus entices victims to download malicious apps from the Google Play Store. It then gains administrative privileges, records keystrokes, intercepts/hides F2A SMS communications, and accesses mobile banking and cryptocurrency apps to transfer funds. SharkBot has targeted five different cryptocurrency providers and international banks from the United Kingdom and Italy.

### The United States is Expected to Hold the Major Share in the North American Region

The United States is considered the most prominent market for cybersecurity insurance in the world. The country is also home to

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

a significant number of key players operating in the market, which is another reason for the country's high share. Cyberattacks in the United States are rising rapidly and have reached an all-time high, primarily owing to the rapidly increasing number of connected devices in the region. In the United States, consumers are using public clouds, and many of their mobile applications are preloaded with their personal information for the convenience of banking, shopping, communication, etc. According to the White House Council of Economic Advisers, the US economy loses approximately USD 57 billion to USD 109 billion per year to harmful cyber activity. To minimize this loss due to cyber attacks, the solutions offered by cyber security insurance providers are essential, and the demand for cyber security insurance is increasing in the region. The region has been witnessing a significant number of data breaches over the years. According to the report published in 2022 by the Identity Theft Resource Center, 1,789 data breach incidents have been recorded. The high number of data breaches encourages organizations across various industries to opt for cybersecurity insurance, driving the market's growth. The United States government signed the law to establish Cybersecurity and Infrastructure Security Agency (CISA) to enhance the defense against cyber attacks. It works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the governmental networks that support essential operations of the partner departments and agencies. As a result, it will open new avenues for the new and existing companies to invest in suitable cyber security suite designed for this industry. In August 2021, T-Mobile, a mobile telecommunications company in the United States has announced that its systems were attacked through an unprotected network access device in July. By August, the attacker gained direct access to the servers containing account and personal information on former, current, and prospective account holders. Moreover, the company confirmed an additional compromise in late December 2021 that impacted an undisclosed number of customers.

#### Cybersecurity Insurance Market Competitor Analysis

The cybersecurity insurance market is moderately consolidated, with significant players offering superior technology and fostering growth through their existing distribution channels. These technology leaders are investing in innovations, mergers, acquisitions, and partnership activities to maintain a competitive edge in the market.

October 2021 - Lockton launched the Silent Cyber Property Solution. This stand-alone policy protects the client's business against property damage and the loss of time due to cyberattacks or cyber terrorism. Insurance buyers can purchase up to USD 150 million in program limits per outbreak, with the potential for additional market capacity as needed.

August 2021 - With instances of ransomware attacks increasing, AON and Crawford pooled their combined cyber experience and produced a detailed guide to help organizations better mitigate cyber risks and manage insurance claims more effectively in an incident. The guide examines how advances in cyberattacks, particularly ransomware, resulting in rapid inflation in loss frequency and severity while simultaneously increasing the complexity of managing the impact of business interruption.

May 2021 - Japan's Mitsui Insurance invested USD 36 million and made a strategic partnership in Israel's Upstream Security as part of the startup's C funding round. The partnership would enable the Japanese insurer to employ Upstream's machine learning and analytics capabilities to derive insurance insights from mobility data. MSI and Upstream will work together to put the power and advantages of automobile telematics data in the hands of Japanese insurers and policyholders.

#### Additional Benefits:

The market estimate (ME) sheet in Excel format  
3 months of analyst support

#### Table of Contents:

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

## 1 INTRODUCTION

### 1.1 Study Assumptions and Market Definition

### 1.2 Scope of the Study

## 2 RESEARCH METHODOLOGY

## 3 EXECUTIVE SUMMARY

## 4 MARKET INSIGHTS

### 4.1 Market Overview

### 4.2 Industry Value Chain Analysis

### 4.3 Industry Attractiveness - Porter's Five Forces Analysis

#### 4.3.1 Threat of New Entrants

#### 4.3.2 Bargaining Power of Buyers

#### 4.3.3 Bargaining Power of Suppliers

#### 4.3.4 Threat of Substitute Products

#### 4.3.5 Intensity of Competitive Rivalry

### 4.4 Industry Guidelines and Policies

### 4.5 Assessment of the Impact of COVID-19 on the Market

## 5 MARKET DYNAMICS

### 5.1 Market Drivers

#### 5.1.1 Increasing Adoption of Cloud-based Services

#### 5.1.2 Rising Data Security Breaches

### 5.2 Market Restraints

#### 5.2.1 Difficulties in Implementing Cyber Insurance and High Costs

## 6 MARKET SEGMENTATION

### 6.1 Organization Size

#### 6.1.1 Small and Medium Enterprises (SMEs)

#### 6.1.2 Large Enterprises

### 6.2 End-user Industry

#### 6.2.1 Healthcare

#### 6.2.2 Retail

#### 6.2.3 BFSI

#### 6.2.4 IT and Telecom

#### 6.2.5 Manufacturing

#### 6.2.6 Other End-user Industries

### 6.3 Geography

#### 6.3.1 North America

##### 6.3.1.1 United States

##### 6.3.1.2 Canada

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.3.2 Europe
  - 6.3.2.1 Germany
  - 6.3.2.2 United Kingdom
  - 6.3.2.3 France
  - 6.3.2.4 Rest of Europe
- 6.3.3 Asia-Pacific
  - 6.3.3.1 India
  - 6.3.3.2 China
  - 6.3.3.3 Japan
  - 6.3.3.4 Singapore
  - 6.3.3.5 Rest of Asia-Pacific
- 6.3.4 Rest of the World

## 7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
  - 7.1.1 XL Group Ltd
  - 7.1.2 American International Group Inc.
  - 7.1.3 Berkshire Hathaway Inc.
  - 7.1.4 Zurich Insurance Co. Ltd
  
  - 7.1.5 The Chubb Corporation
  
  - 7.1.6 Aon PLC
  - 7.1.7 Bin Insurer Holding LLC
  - 7.1.8 Lockton Companies Inc.
  - 7.1.9 Security Scorecard Inc.
  
  - 7.1.10 Allianz Global Corporate & Specialty
  - 7.1.11 Munich Re Group

## 8 INVESTMENT ANALYSIS

## 9 MARKET OPPORTUNITIES AND FUTURE TRENDS

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Cybersecurity Insurance Market - Growth, Trends, Covid-19 Impact, and Forecasts  
(2023 - 2028)**

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

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	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-01"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)