**Cybersecurity Insurance Stats**

**How Big is the Cybersecurity Insurance Market Globally?**

According to [Research and Markets](https://www.researchandmarkets.com/reports/5636783/global-cyber-insurance-market-forecasts-from?utm_source=CI&utm_medium=PressRelease&utm_code=d8pdbw&utm_campaign=1749248+-+Global+Cyber+Insurance+Market+to+Reach+%2420.43+Billion+by+2027&utm_exec=como322prd), the global market size for cyber insurance was USD 7.06 billion in 2020 and is expected to grow to USD 20.43 billion by 2027. In 2021 ([Fortune Business Insights](https://www.fortunebusinessinsights.com/cyber-insurance-market-106287)), the cyber insurance market was USD 7.49 billion globally. Both studies predict that the market will grow at a CAGR of 24% over that same time.

**How Big is the Cybersecurity Insurance Market in the US?**

The US market continues to be the largest contributor to the cyber insurance market, with a total market cap in 2020 of USD 2.38, according to an article on [Fortune Business Insights](https://www.fortunebusinessinsights.com/cyber-insurance-market-106287). Further, it is predicted that the US will continue to be the largest driver in the growth and adoption of cyber insurance over the next 6 years.

**Is the Cyber Insurance Market Growing?**

The short answer is yes, the market is growing, but like many markets over the last few years, COVID-19 has introduced unforeseen factors that have altered the growth pattern and adoption. [Fortune Business Insights](https://www.fortunebusinessinsights.com/cyber-insurance-market-106287) analysis shows that cybercrime and claims are increasing across the globe, which further drives the adoption and desire to have coverage for cyber-related incidents. Other factors that are contributing to the adoption and growth, according to IBM reference in the [Research and Markets](https://www.researchandmarkets.com/reports/5636783/global-cyber-insurance-market-forecasts-from?utm_source=CI&utm_medium=PressRelease&utm_code=d8pdbw&utm_campaign=1749248+-+Global+Cyber+Insurance+Market+to+Reach+%2420.43+Billion+by+2027&utm_exec=como322prd) report, is that the overall cost of claims is going up.

**Analysis of the market and growth:**

While these numbers seem to be supported across multiple studies, there is room to theorize that the overall growth in the industry may be stronger in that period. From personal experience and from conversations with peer CISOs across industries, overall rates and ability to gain cyber insurance are becoming more difficult. To me, this indicates a demand that is stronger than the risk appetite of the insurers and shows that organizations are utilizing cyber insurance as a mechanism to help make the organization whole, in the event of a breach.

I have heard from several CISOs and executives that have claimed to be turned away by cyber insurance carriers. In some cases, this may be due to the type of business or vertical the organization operates within. This is very similar to trying to get homeowners’ insurance in a hurricane-susceptible region or a low natural disaster region with a fire station close by. The risk of loss to the insurer is lower. This further indicates to me that the market is extremely strong and has high demand, as it was not that long ago that almost any organization could get coverage if they chose; no matter how good their security program was.

**How Common is Cyber Insurance? (Ie stats on what percentage of companies have it and what kind of companies these are)**

It can be difficult to know just how many organizations have coverage and what level of coverage they have, as this data is self-reported. However, in an article by [The Register](https://www.theregister.com/2022/08/11/insurance_ransomware_blackberry/), of 450 organizations surveyed, only 19% claimed to have coverage for cyber events beyond $600,00 with a total of 55% having coverage at all. Another way to look at total adoption is based on the total written coverages and according to a report published by [NAIC](https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf) in 2021. The total number of written premiums in 2020 was USD 2.7 billion with a total policy in force of 4 million. Additionally, in this report, we can see continued adoption year after year from 2016 (doubling in that time), with the largest increase being from 2019 to 2020.

**How Common Are Cyber Insurance Claims?**

A good way to review the total number of claims is to review the loss ratios. Insurers expect to have to pay out a certain number of the full claims each year, and they attempt to spread that cost across the premiums, in hopes of not having to pay out all of the premiums. In 2020, according to the report published by [NAIC](https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf), the top 20 insurers’ loss ration ranged from 24.6% up to 114%.

According to a [FitchRatings](https://www.fitchratings.com/research/insurance/us-cyber-insurance-payouts-increase-amid-rising-claims-premium-hikes-06-05-2022#:~:text=Cyber%20incidents%20continue%20to%20grow,8%2C100%20claims%20paid%20in%202021.) article, in the past 3 years, cyber insurance claims have increased by an order of 100% and payouts a total of 200%, with the peak claims being 8,100 in 2021. For further details on claims, a great report by [NetDiligent](https://netdiligence.com/cyber-claims-studies/) (NetDigilgence Cyber Claims Study 2021 Report) analyzing 5,797 claims from 2016-2020 can be reviewed, as well. In this study, it was found that 99% of all claims came to SME companies (annual revenue under $2 billion).

**What is The Average Cyber Insurance Claim? ($)**

Referencing the report by [NetDiligent](https://netdiligence.com/cyber-claims-studies/) (NetDigilgence Cyber Claims Study 2021 Report), ransomware continues to be the most common cyber insurance claim followed by phishing attempts. However, it can be argued that phishing is the primary culprit of compromise, as this is how most ransomware is entering the business.

An article by [Security.org](https://www.security.org/insurance/cyber/statistics/) further highlights a few key statistics when it comes to claims. One in six claims were related to ransomware, the FBI saw an increase of 69% of reported complaints or crimes in 2020. Also, a total of 37 billion personal records were compromised in 2020, which shows that the impact and the total number of breaches are not slowing down. All of this can be evidenced by additional legislation and regulatory requirements that are being passed and required for organizations.

**What is the Most Common Reason for a Cyber Insurance Claim? (ie which type of incident most commonly leads to a claim)**

Utilizing the report by [NetDiligent](https://netdiligence.com/cyber-claims-studies/) (NetDigilgence Cyber Claims Study 2021 Report) to break down the insurance claims, the SME average claim cost is $111k for crisis services, $98k for legal, and $145k for the incident itself, with an average of $345k. However, when it comes to ransomware, the total average costs rise to $485k.

**What Percentage of Security Breaches Are Covered by Cyber Insurance?**

In a report produced in 2021 by [Willis Towers Watson](https://d.docs.live.net/be3528fbca6bc620/Downloads/Cyber%20claims%20analysis%20report%20-%20WTWhttps:/www.wtwco.com%20›%20WTW%20›%20Insights%20›%202021/03), you can find a chart that breaks down the cost of claims by type and how the event was paid. In 36% of the events the insurer paid under the policy limit, and in 2% of the average loss that was covered was not covered. In all, 27% of data breach claims and 24% of first-party claims had some exclusion written into the policy that prevented payout or full payout.

**Who Are The Largest Cybersecurity Insurers? (who are they? How big compared to close competitors etc)**

The top 8 cybersecurity insurers, according to [eSecurity Planet](https://www.esecurityplanet.com/products/cyber-insurance-companies/), are AXA XL, Chubb, AIG, Travelers, AXIS, Beazley, CAN, and BCS. What is more astounding is that AXA XL, Chubb, AIG, and Travelers make up 40% of the market for policies across all industries. With so few having such a large percentage of the market, they really can dictate the rates and increase, along with requirements for insurance. However, they are also taking on a larger percentage of risk and loss at the same time.

**What’s The Most Popular Type of Cyber Insurance? (eg standalone policy? Combined with general policy? Other?)**

There are multiple types of cyber security insurance an organization can have. [Beazley](https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response.html?utm_medium=paid_search&utm_source=google&utm_campaign=Cyber_NonBranded&utm_content=NB_CyberInsurance&gclid=CjwKCAjwp9qZBhBkEiwAsYFsbxAz9qKXEFmLdbTpzBtaMq9n8i6OuKE2vwEpU8RC7ciHnoJEqBmagRoC408QAvD_BwE) lays out the most common types of policies that are available. Ranging in coverage and use cases, you have policies for breach that covers response, investigations, and monitoring services. There is the first party, which includes business interruption, extortion, and recovery costs. Also, there is third-party coverage that helps with regulatory fines, privacy, and media. An additional policy can be added to the writer that covers fraud, which could be an accident transfer of funds or other fraudulent activities.

While it would be great to have hard numbers on which policies are most popular, through searching, I was not able to find a solid article that provided this information. Rather, I will refer to the report by [NetDiligent](https://netdiligence.com/cyber-claims-studies/) to infer what coverage companies most often cover. Based on the cost of the breaches, it would appear the two most common policies carried out are breach response and first-party insurance. Speaking from experience and from what I hear from peer CISOs, fraud insurance can be hard for any business that deals with payments (either business or consumer) regularly, so this policy tends to be utilized less. Further, it is common for policies to be written with a primary and secondary provider, usually split evenly to help offset the risk exposure.

**Most Popular Reason Companies Invest in Cyber Insurance? (Is it for compliance purposes? To help with gaining new business? Fear of a breach? Something else)**

Pulling from a [Travelers](https://www.travelers.com/cyber-insurance/4-ways-cyber-insurance-helps-protect-your-business) article, the most common reasons that a company will have cyber insurance is as follows: lost data, lost devices, notification requirements, and forensics. Recovering from an incident can be costly, especially when systems need to be restored or rebuilt because they have been compromised and are not able to operate safely. Additional regulatory requirements and fines have increased the cost of a breach, due to fines that can be levied against an organization. Often, each compromised or deleted record is charged several hundred dollars. For an organization to be able to withstand the financial hit, the organization will need insurance to assist with the costs of dealing with a breach and the fines that will result from it.