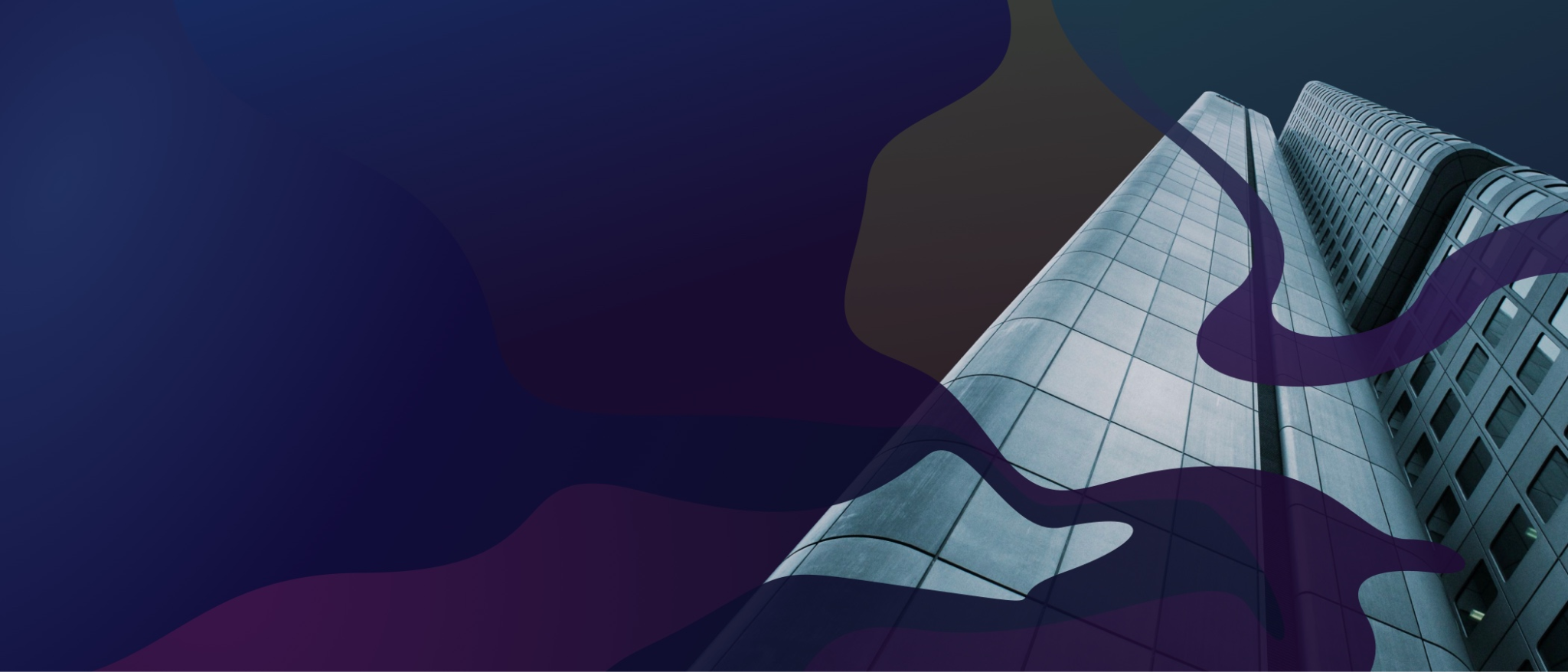
# **Cyber Insurance: Overview**



## **Cyber insurance is becoming an important tool in the corporate incident response arsenal**

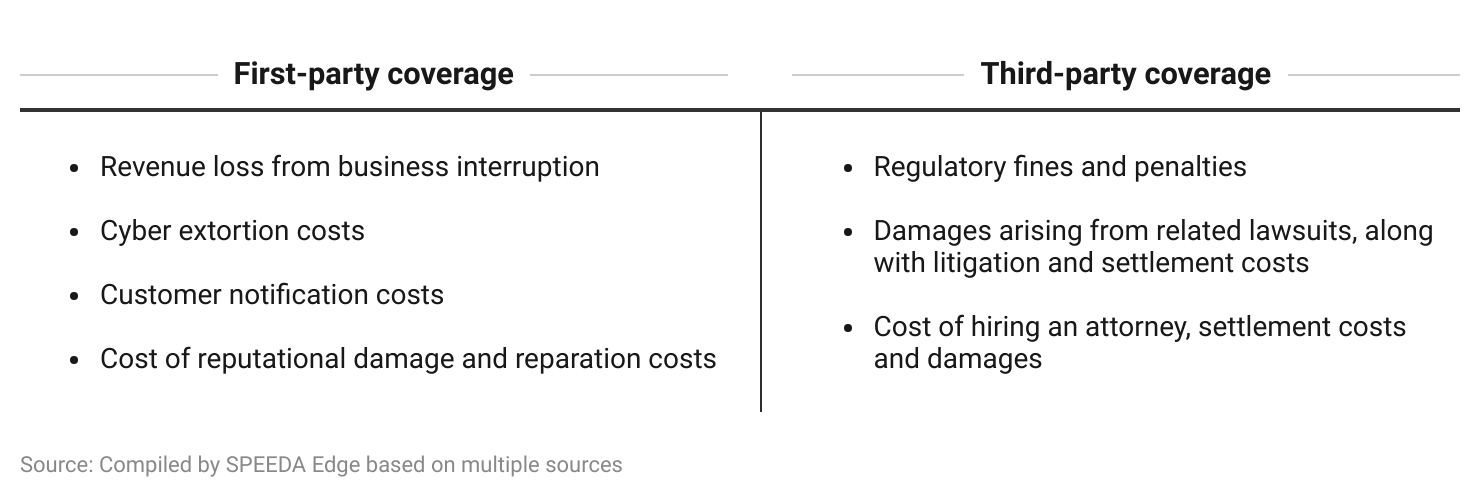
Cyber insurance is a specialty insurance product that protects organizations from liabilities arising from cybersecurity incidents. General liability insurance policies for enterprises provide little to no coverage for cybersecurity events, giving rise to specialized insurance products to cover these liabilities.

#### **Policies cover first- and third-party damages, usually under an agency model**

A cyber insurance policy typically provides coverage against first- and third-party liabilities. First-party liabilities are those incurred by the company that carries the insurance policy, while third-party liabilities refer to claims made by external parties because of cybersecurity incidents.

### 

### **Liabilities covered under a typical cyber insurance policy**



Most startups that offer cyber insurance operate under an agency model, where they issue policies that are underwritten by a larger insurer/reinsurer, although several prominent players in the space have recently started writing their own insurance policies and adopting a full-stack insurer model, usually through the acquisition of a fully admitted carrier. Some cyber insurance providers also offer coverage for technological errors and omissions (E&O)—a special policy that protects companies (mainly in tech) against legal liabilities arising from errors in the products they sell.

## **Cyber insurance is not a substitute, but part of a wider cyber defense strategy**

While sophisticated cybersecurity products exist to help businesses detect and respond to cyber threats, no strategy provides complete protection against motivated cybercriminals. The recent increase in cyber attacks and associated monetary damages are pushing enterprises to consider cyber insurance as an essential part of their incident response kits. This is more significant for small businesses, as they often lack the expertise and resources to recover from such an attack.

Cyber insurers take a preventative approach to insurance, and policies are tailored to an organization’s security posture, using risk assessment tools that leverage AI. They often come bundled with solutions that allow proactive monitoring to identify security issues within the insured’s infrastructure. They give the insurer the ability to monitor their own portfolio risks while assisting in incident response.

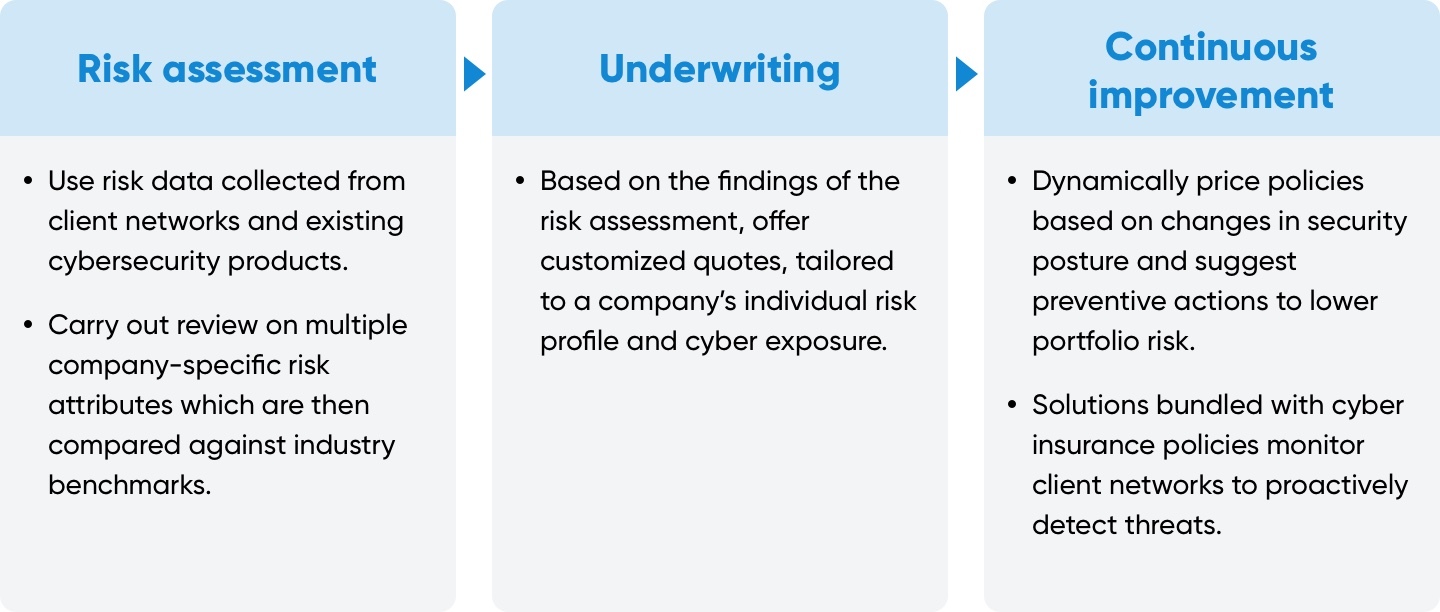
Insurance policies and bundled offerings are just one part of an organization’s overall cyber defense strategy. They are not intended to replace the threat detection capabilities of a fully-fledged cybersecurity solution or a company’s own cybersecurity practices. At the time of policy issuance or renewal, insurers require companies to have a sound cyber defense framework in place, with their current security posture being pivotal in determining premiums. Some insurers go to the extent of declining coverage for companies that fail to demonstrate the required levels of cyber hygiene.

## **Cyber insurers leverage AI and machine learning to assess dynamic risk landscape**

AI and machine learning (ML) have enabled digital means of assessing cyber risk. These tools can automate enterprise infrastructure scanning, carry out risk ratings, and estimate the financial impact of cyber risk prior to onboarding, resulting in a more accurate underwriting process.

Even after the policy is issued, bundled solutions help insurers with continuous portfolio monitoring, as they scan client networks in real-time and alert them to potential risks. This creates a continuous feedback loop between the client and insurer, allowing the latter to dynamically price insurance policies. It also allows insurers to take on a more active role in client security by proactively monitoring client infrastructure and suggesting preventive measures, resulting in lower overall portfolio risk.

### **How AI/ML helps insurers manage cyber insurance portfolios**

****

Source: Compiled by SPEEDA Edge based on multiple sources

More recently, generative AI (GenAI) has seen some use in the cyber insurance space to support underwriters and policyholders. This includes AI assistants that allow users to ask questions on cyber and management strategies, AI-driven search functions, and AI-powered tools that act as information sources for brokers and policyholders to query insurance policy information and processes.

## 

## **The cyber insurance landscape**

We identify four types of startups in the cyber insurance industry hub: 1) pure-play cyber insurers, 2) commercial insurers, 3) risk assessment and rating platform providers, and 4) cyber risk modeling platform providers.

Startups that provide insurance—either as a pure play provider or as part of a commercial insurance offering—generally operate on a hybrid model where they provide insurance as well as bundled cybersecurity solutions. They also have partnerships with other cybersecurity vendors to allow their clients to obtain discounts on more sophisticated products.

Cyber insurance providers have teams that comprise individuals from both cybersecurity and insurance backgrounds, who help clients with proactive monitoring and incident response. Disruptors across insurance provider segments have maximum coverage limits in place to control their risk exposure, with upper limits in the range of USD 10 million to USD 15 million. This is usually combined with revenue criteria, further limiting the disruptor’s exposure to larger and more vulnerable enterprises.

Risk assessment startups provide solutions for insurers and brokers to support their risk assessment procedures to underwrite cyber risks. For instance, Security Scorecard has partnered with incumbent insurers such as AXA and Liberty Mutual to support their underwriting functions.



# 

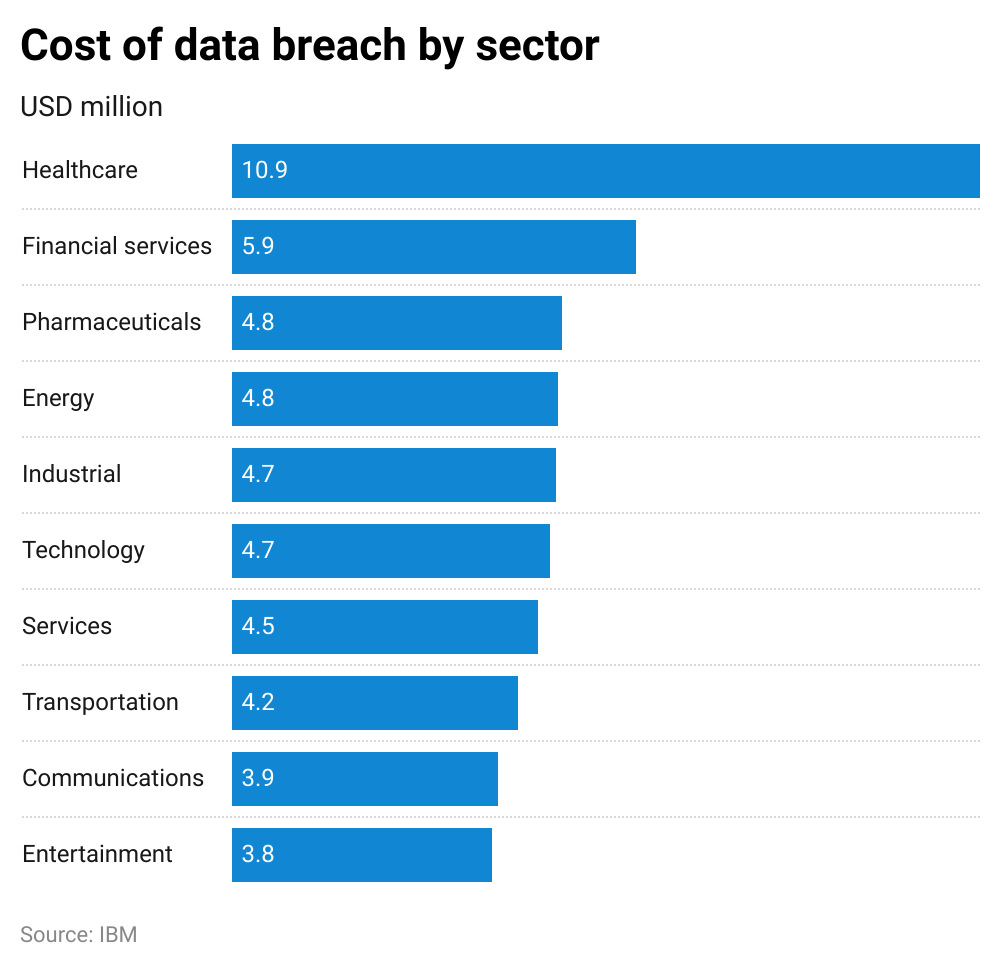
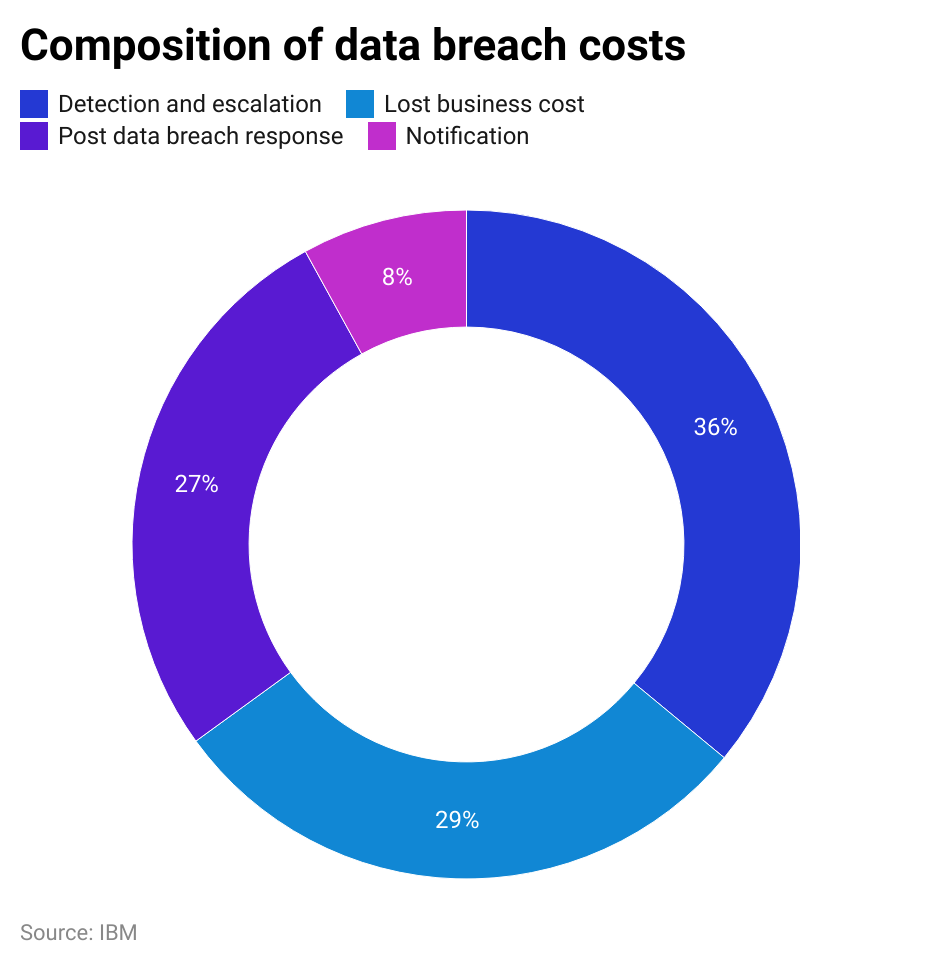
# **Driving factors**

## **1. Millions at stake with data breaches and ransomware attacks on the rise**

We witnessed a record 3,205 publicly reported data breaches and other compromises of personal information in 2023, reflecting a 72% increase compared to the previous all-time high of 1,860 in 2021.

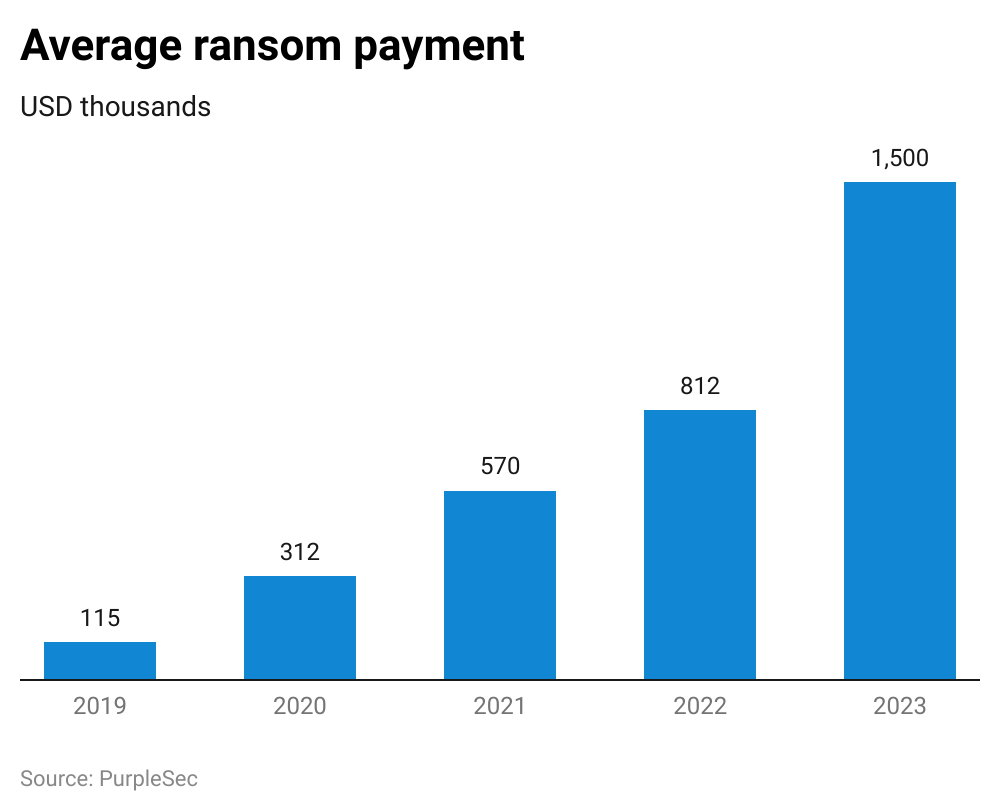
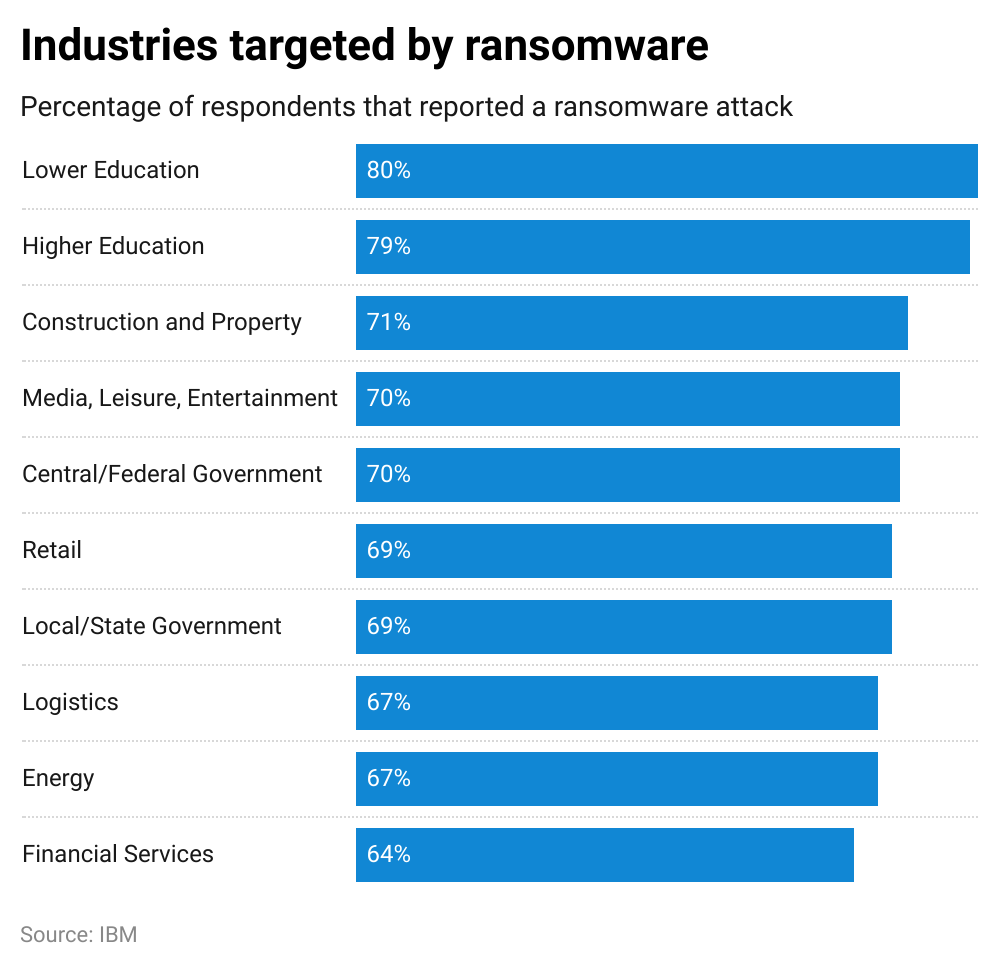
The average cost of a data breach in the US amounted to USD 9.5 million between March 2022 and March 2023, more than double the global average of USD 4.5 million. Detection and escalation accounted for the largest component of data breach costs, followed by lost business costs. Post-incident response accounted for 30% of these costs and included issuing new accounts, product discounts, legal expenses, and regulatory fines.

The healthcare sector has been the most susceptible to cyber attacks, with nearly one out of every four data breaches stemming from it in 2023. The sector also accounted for the highest average data breach cost in 2023, amounting to USD 10.9 million.



Ransomware attacks were the second largest cause of data breaches and are ubiquitous across multiple industries. In 2023, more than 75% of companies in the US struck by ransomware reported paying the ransom. This, combined with the relative ease of accessing ransomware kits, has resulted in attack volumes growing 95% YoY in 2023.

The average ransom payment in 2023 amounted to USD 1.5 million—nearly double the average in 2022. The overall impact of ransomware attacks goes beyond just the ransom payment. Estimates placed the overall damages, accounting for associated costs such as business disruption and reputational harm, at USD 42 billion globally in 2024.



On average, a cyber insurance premium ranged between USD 672 and USD 1,788 per annum in 2024 depending on the policyholder’s industry, with liability limits ranging from USD 1 million to USD 5 million. The cost of cyber insurance policies varies based on the type and size of the company, the industry it operates in, its exposure to cyber risk, and coverage limits. For instance, a hospital with a coverage limit of USD 10 million, can pay up to USD 247,000 per year in premiums. Given the uncertainty and large potential payouts, cyber insurance policies are among the highest in terms of premiums per USD million of coverage, second only to commercial auto insurance.

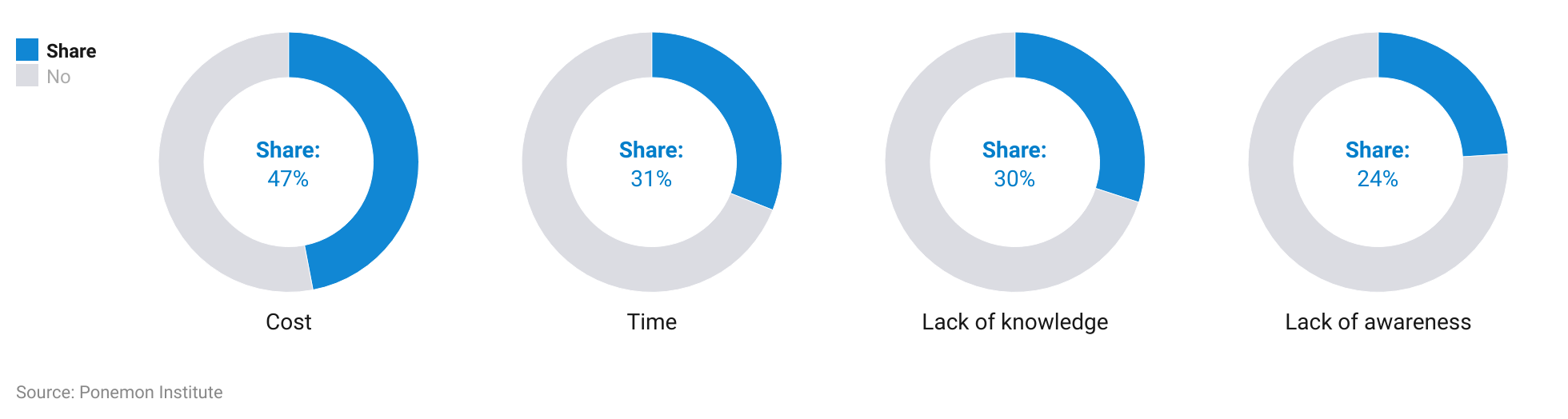
### **Approximate cost for USD 1 million of coverage limit**



## **2. Small businesses in the crosshairs, but lack resources for effective cyber defense**

More than 73% of small and mid-sized businesses (SMBs) in the US reported a cyber attack in 2023; over half cited inadequate budgets as an impediment to effective cybersecurity postures. SMBs also report a lack of knowledge and awareness around cyber threats and security solutions, insufficient time, and the absence of in-house expertise, as other reasons. According to a 2022 analysis, 60% of businesses affected by a cyber attack go out of business within six months, and 75% of SMBs hit by ransomware say they would not be able to continue operating. Furthermore, 51% of small businesses reported downtime of 8–24 hours, and 40% reported losing critical data in a cyber attack.

### **Challenges for SMBs in ensuring effective cybersecurity posture**



Cyber insurance policies, with their bundled solutions and teams, help address some of the security posture gaps of SMBs. For instance, insurance provider Corvus Insurance offers a virtual Chief Information Security Officer (vCISO) that allows companies to consult with Corvus’ in-house experts. The company also allows insureds to obtain cybersecurity solutions from select partners at concessionary rates. A 2019 survey on small businesses with cyber insurance indicated that 70% of such companies get help from their insurers to mitigate cyber risk. This indicated that though cyber insurance is a response tool, smaller businesses are able to leverage the bundled offerings to improve their cyber risk management practices.

## **3. Unpredictable cyber threats call for sophisticated methods to assess risk**

Traditional insurance markets, such as automobiles and property, have a lot of historical information available on the frequency and severity of loss events, which is used to price insurance policies. However, given its infancy, the cyber insurance industry lacks sufficient volumes of historical data.

While reviewing historical data is not without merit, relying solely on it and other traditional approaches, such as manual questionnaires, will not adequately capture the cyber risks a company will face. This is due to the dynamic nature of cyber insurance, where factors such as the organization’s security posture, the industry it operates in, the type of attack, and the extent of the loss, can vary significantly across individual incidents.

The timing and severity of a cyber attack cannot be reliably predicted. This has increased demand for AI-based solutions that leverage an insurer’s internal data and external information, such as industry standards, to automatically benchmark enterprise networks and assess cyber risk efficiently. It also quantifies the financial impact of these risks. Startups are providing AI-based solutions to meet this need, which helps cyber insurance brokers and underwriters come up with pricing that accurately reflects the risk potential, which in turn can translate to lower loss ratios. It also helps them stay on top of a client’s security posture on an ongoing basis and suggest remedial action when needed.

# **Risks to growth**

## **1. Lack of standardization and awareness on cyber risk exposure keep buyers at bay**

Insurance policies from different providers are likely to have varying terms and features, making it difficult for potential buyers to compare insurance options. This also instills fear among buyers who may not be clear about exclusions at the onset, only to discover coverage gaps at the time of making a claim. Companies, especially the larger ones, are also concerned about whether the coverage options on offer are sufficient for their risks, given that most policies are currently capped at relatively low limits.

Small businesses, in spite of increasingly falling victim to cyber attacks, still underestimate their exposure, with 36% of those in the US not being concerned about falling victim to a cyber attack and 59% of small businesses with no cybersecurity measures in place believing they are too small to be attacked. 70% of small business owners believe they were prepared to defend against cyber attacks and recover from breaches. The inability to properly understand risk exposure also results in buyers not being able to determine how much insurance coverage they need and, therefore, lowering take-up.

## **2. Having cyber insurance could encourage more attacks, forcing insurers to re-evaluate business models**

In the event of a ransomware attack, companies that have cyber insurance are more likely to pay the ransom to minimize business disruption. This encourages cybercriminals to execute more attacks on such companies.

Ransomware was involved in nearly 20% of cyber insurance claims in the first half of 2023.. The high values of these ransom payments pose significant profitability challenges for the industry. It also worsens a situation where demand significantly exceeds the supply and the market capacity to write cyber insurance. Loss ratios for cyber insurance policies in the US amounted to 73%—the highest in six years. Some incumbent insurers, such as AIG and CNA, were actually losing money on their cyber policies. As a result, insurers are becoming stricter and more selective in their underwriting, while adding more exclusions to remain sustainable. In May 2021, incumbent insurer AXA went to the extent of stopping ransomware coverage altogether in its cyber insurance policies in France. Carriers are also looking at increasing premiums, with some demanding a 50% hike at renewal to reflect the growing cyber risks.

*Last updated: March 2024*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.