

## Cost Trend

# Cyber Insurance Rates Ebb, Insurers Add Exclusions



**RAPID REACTION FORCE:**  
Businesses are reacting more quickly to breaches, which can minimize the damage.

**W**HILE CYBERATTACKS continue to grow in number, the cost of cyber insurance has been dropping thanks to businesses implementing better controls to thwart such activity and reduce their losses if they become victims of a malicious attack, according to a new report.

Rates fell an average of 17% last year after surging in 2021 and 2022 as the COVID-19 pandemic spurred cyber criminals to ramp up attacks, according to insurance group Howden's 2024 cyber report. The trend has continued in 2024, yet at a slower clip.

Another report found that rates fell 5% in the second quarter, compared to the same period in 2023.

Premiums have declined despite ransomware attacks growing an eye-popping 218% year-on-year in 2023. But, fewer ransomware victims (just 17% according to one report) are paying the ransom as businesses have implemented stronger risk controls that keep an attack from posing an existential or costly threat to them.

## Factors affecting rates

While the number of cyber claims grew 65% in 2023, according to a report by Aon, businesses have gotten better at detecting, quarantining and shutting down attacks, as well as reacting quickly if their systems are breached. This has reduced the cost of claims when they are filed.

Employees have also been better trained to detect malicious e-mails and avoid clicking on the types of links that can release a malware, ransomware or other code, thus thwarting attacks that could be costly.

Companies have also been able to reduce their business interruption costs after a cyberattack by employing better back-up systems, such as through cloud providers.

Also, more insurers have entered the cyber insurance market, which has increased competition and helped tamp down pricing

Some analysts, however, attribute the rate hikes to a blip, pointing to growing numbers of ransomware and business e-mail compromise scams, attacks that may spur rate hikes again. And they point to evolving threats, like artificial intelligence and the threat of cyber warfare in an increasingly volatile world.

## New exclusions

Cyber insurers continue adding new exclusions to their policies. Some new ones that you should be aware of include:

**War risk and systemic risks** – Volatile geopolitics have spurred cyber insurers to expand exclusions around war and they are imposing sub-limits for other systemic events.

**Regulatory** – Some cyber insurers are also restricting coverage for regulatory risks due to increasing claims and costs like investigations, settlements, fines and penalties.

**Wrongful data collection** – With more state, federal and even foreign laws barring website owners from collecting certain kinds of data without the permission of website users, businesses have great exposure to actions by regulators and government prosecutors.

As a result, more cyber insurers are also restricting coverage of costs related to a business being hit with fines, penalties or legal action for breaching data privacy laws.

## The takeaway

Businesses need to continuously be vigilant against the always present threat of cyberattacks.

When it's time for renewal we recommend that you meet with us to discuss your potential exposure. Every company has a different risk picture.

And considering the increasing use of exclusions, we can help you cut through the policy language to look for changes that may increase exclusions and restrict coverage of certain events. ❖