everest®

We underwrite opportunity.™

The State of the Cyber Insurance Market 2023

ZYWAVE

everest®

Table of Contents

Introduction

Price changes, policy wording debates, and a roller coaster of cyber threat shifts – the global cyber insurance industry has dealt with these challenges and more over the last several months. To better understand the forces driving today's market, Everest Re and Zywave collaborated on a survey of cyber insurance participants – brokers, underwriters, and incident response professionals. The results offer a snapshot of a dynamic market still grappling with growing pains but well on its way to maturity.

Key Takeaways

- Rate adequacy for primary and excess cyber has nearly **80% of underwriters** concerned.
- Brokers feel underwriters are maintaining underwriting discipline. Underwriters, feeling the competitive pinch, view it a little differently.
- **It's a broker's market**, say 78% of underwriters, who say competition from new and existing players has ramped up significantly and they have far less leeway on coverage or price.
- More underwriters believe that a future standard cyber insurance policy will contain several exclusions aimed at managing aggregation risk, while brokers felt differently.
- Most underwriters are working on **modernized war exclusions** and support them as a long-term strategy – but still have frustrations around the policy-making process. Brokers are far less supportive of the modernized versions.
- The market still has ways to go to reach maturity, but respondents feel it's getting there.

Pricing

Without a doubt, excess pricing took a hit in 2023. We asked respondents to comment on the rate changes over the past three months.

For primary business, 49% indicated overall rate increases over the past three months. However, for excess business, we saw the opposite as 44% of respondents noted rate decreases in the past three months, with the bulk noting the decreases in the 10%-30% range.

In the past 3 months, have you seen cyber insurance rates on **primary policies** average out to about:

- **16%** Increases of over 10% on primary
- **33%** Increases of 0-10% on primary
- **13%** Flat on primary
- **28%** Decreases of 0-10% on primary
- **9%** Decreases of over 10% on primary

In the past 3 months, have you seen cyber insurance rates on **excess policies** average out to about:

- **8%** Increases of over 10% on excess
- **23%** Increases of 0-10% on excess
- **15%** Flat on excess
- **12%** Decreases of 0-10% on excess
- **25%** Decreases of over 10% on excess
- **7%** Decreases of over 30% on exess
- **11%** Don't know/ not applicable

Looking ahead, respondents predicted rate changes in very similar ranges for the next six months, although several comments revealed a close watch on rising loss frequency and severity with a recognition that the tide could – and possibly should – turn in the coming months.

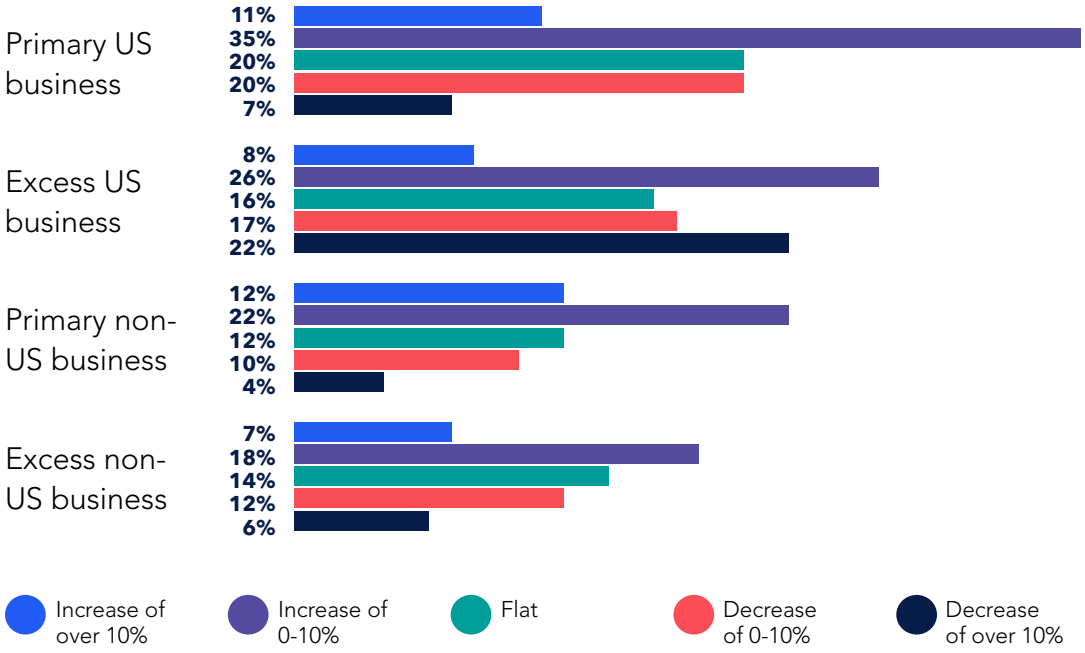
Some respondents noted "decreases could taper off from the effects of MOVEit and other big hacks" and "rates need to stabilize in 2024 as the continued increasing trend of incidents (predominantly ransomware) isn't being commensurately priced for."

Others provided an alternative view, noting that "claims are down overall, and many companies are still competitive and have capacity."

Moderating prices may be welcome news for insurance buyers. They also may attract new and returning buyers, or entice current buyers to buy more limit. In fact, 43% of respondents noted that they are seeing buyers increase their limits at renewal.

However, nearly **60% of respondents** expressed concerns about rate adequacy of both primary and excess covers. If we take a closer look at the answers, underwriters clearly drive the number up with **78% concerned** about rate adequacy on primary and **73% concerned** about rate adequacy on excess.

What do you predict for average rate change in the next 6 months?



One underwriter respondent warned that "losses will tick back up and senior management will once again start noticing the loss activity, how aggressively this business is being written and how much rate has been given back."

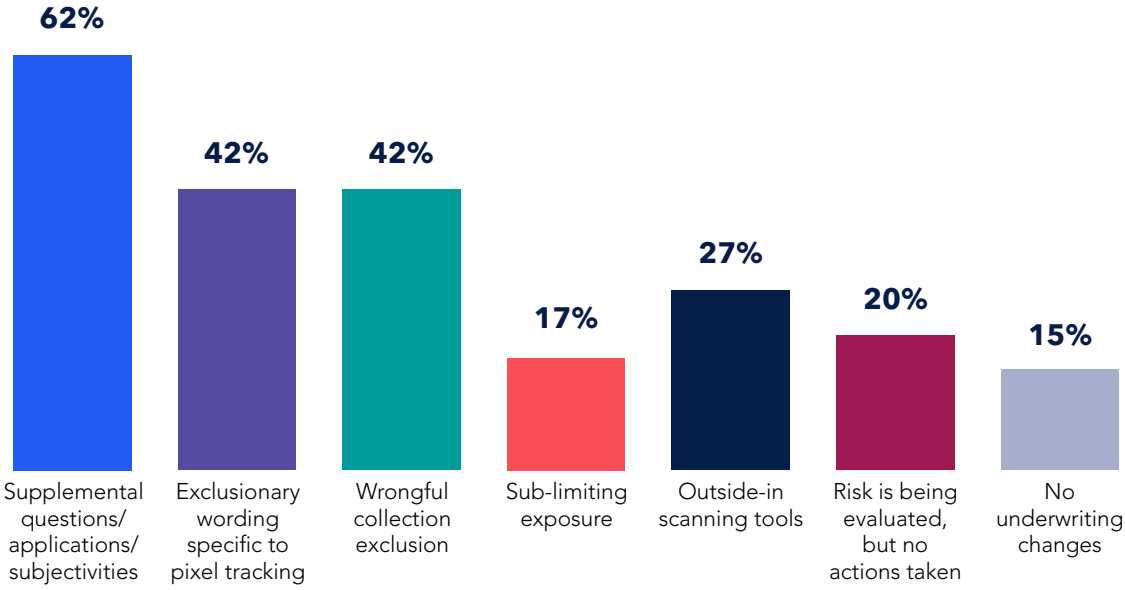
Another had a more optimistic view: "Higher claims activity will push rate[s] up for renewal business but not to the extent of the height of the hard market. Additional capacity and competition will keep rate increases reasonable."

Loss Landscape

The loss landscape also looks different in 2023. We only had a few incident response firms answer the survey, but most of them agreed that they are seeing an uptick from 2022 in ransomware losses and business email compromise losses.

In addition, third-party claims became a hot topic. Exposure to potential pixel tracking claims became a concern and, taking lessons learned from past events, underwriter respondents reported taking action to limit exposure, with 61% using supplemental questions on applications and 34% implementing exclusions for pixel tracking specifically, and 26% excluding the broader risk of wrongful collection.

Are underwriting measures being taken to limit exposure to pixel tracking (e.g. Meta Pixel, Google Analytics, etc.)?



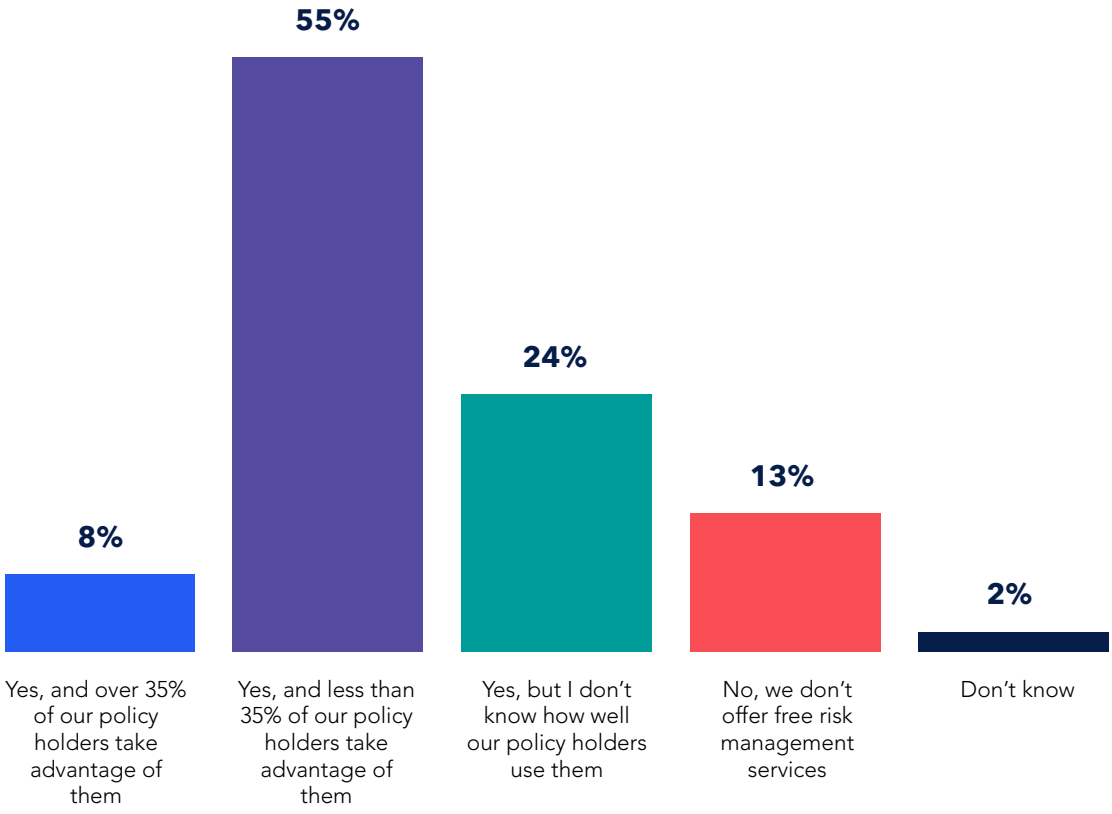
Underwriters' concerns over rising third-party claims aren't unfounded – nearly 50% of respondents said they're seeing an uptick in third-party claims, both data breach and non-data breach related.

Loss Mitigation Strategies

To defend portfolios from losses, 44% of underwriter respondents monitor their portfolios continuously, and 24% monitor at regular intervals. Monitoring was done using third parties (33%), in-house capabilities (31%) and using multiple vendors (22%). Only 14% of underwriter respondents did not do any monitoring at all.

About 85% of underwriter respondents noted that they provided free risk management services with their policies. The take-up rate for those services was low, generally most with under 35% take-up rate. This is despite the free risk management services being ranked an important criterion by brokers for selecting a primary carrier.

Do you offer free risk management services with your policy?

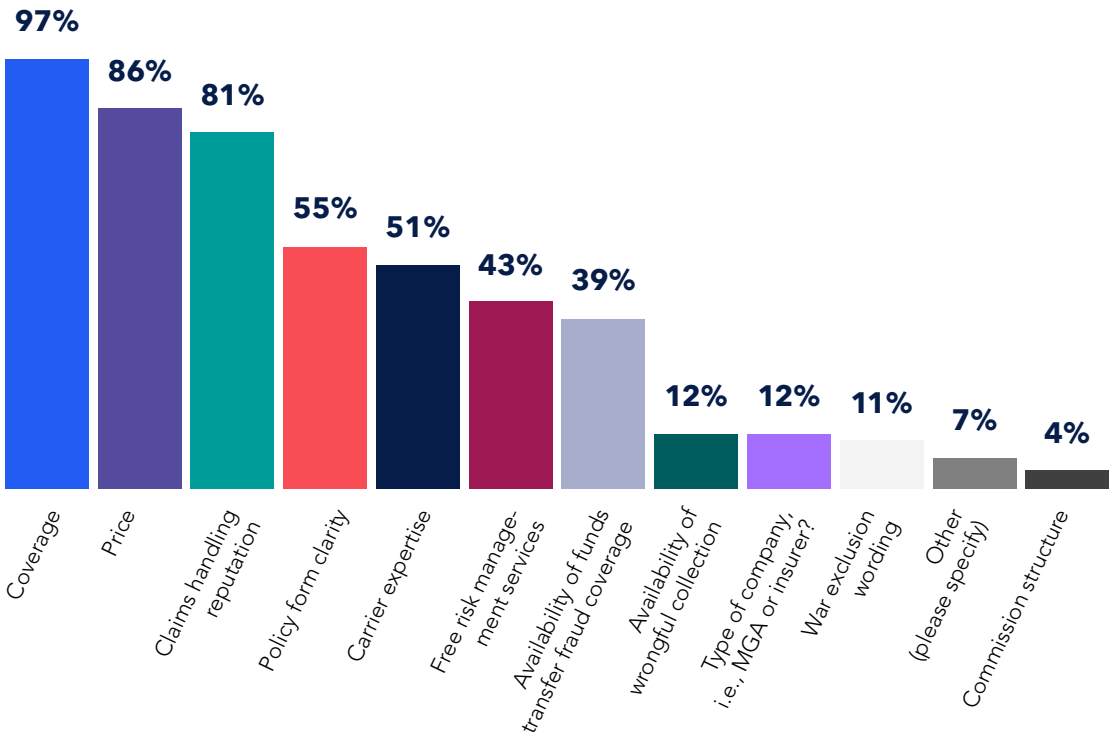


Underwriting

To assist with underwriting, 50% of underwriter respondents use third party underwriting evaluation tools, and 28% developed in-house evaluation tools. Most of these evaluation tools are used to support and evaluate risks but for 43% of underwriters are a very important part of underwriting. Brokers also use risk evaluation tools: 34% use them to prepare their clients for the underwriting process and 37% use them as an additional service provided for their clients.

Brokers consider many different criteria when selecting a primary carrier, the most important of which are, in order: coverage, price, claims handling, policy form clarity and carrier expertise. Some brokers also mentioned choice of vendor panel in their comments. Only 30% of brokers did not feel it was very important to offer options to use off-panel vendors. Underwriters showed some flexibility to offering insureds with choice of vendor panel.

What are the 5 most important criteria for selecting a primary carrier?

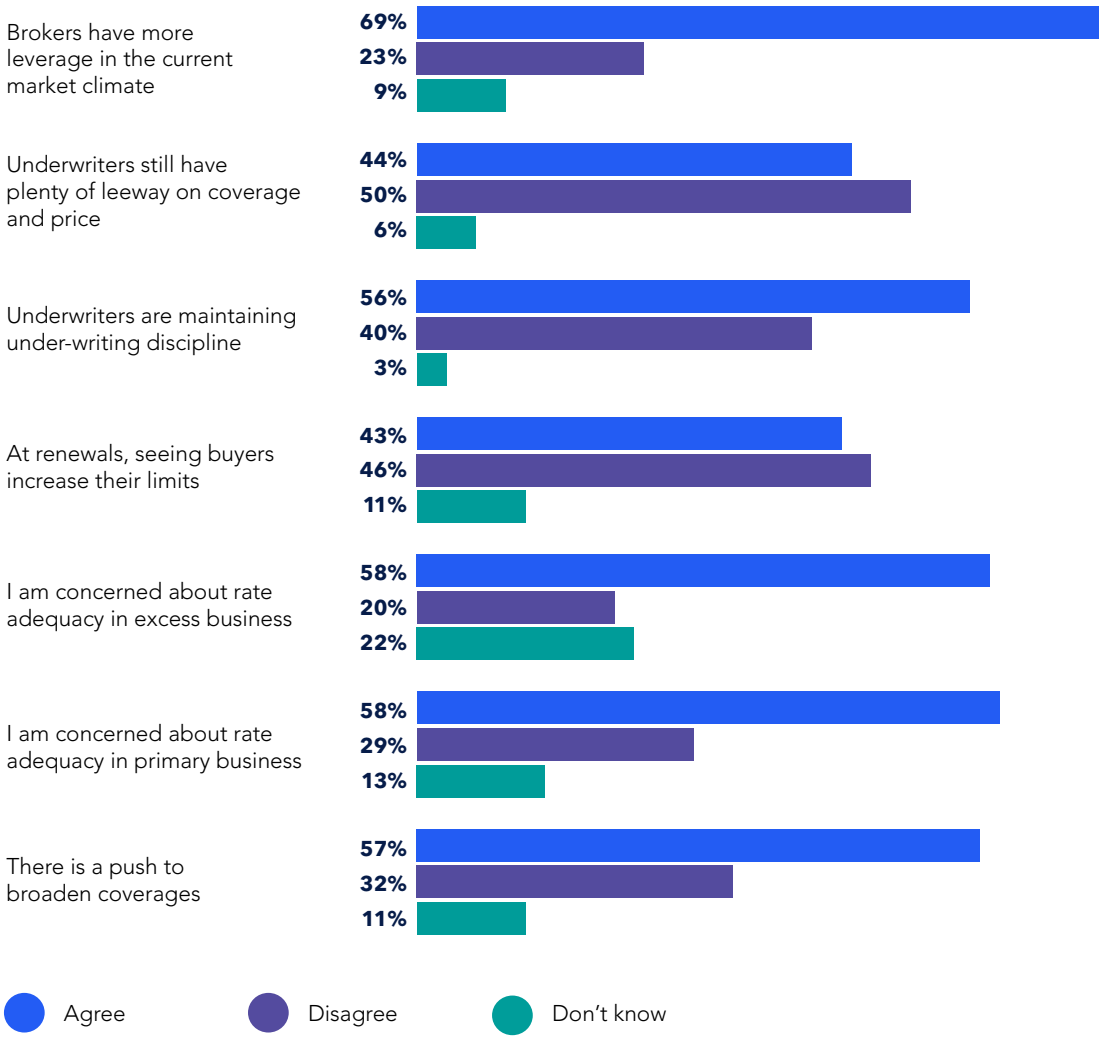


There was a big difference between brokers and underwriters when asked if the underwriters are maintaining underwriting discipline – 75% of brokers agreed with that statement and only 31% of underwriters agreed with it. This discrepancy may be because underwriters are feeling the frustration of a competitive market – in fact 95% of underwriters responded that they see greater competition from existing and/or new players.

Market Dynamics

With all that is going on in the market, it prompts the question – who is in the driver's seat these days for cyber? It's a brokers' market, according to nearly 70% of respondents – most of them underwriters. Furthermore, 55% of underwriters agreed that they were seeing pressure on commissions, and 70% were seeing pressure to offer higher limits in order to compete in the market. All indications that it is a very competitive market.

Please indicate whether you agree or disagree with the following statements.



While brokers display some preference for keeping their clients with the incumbent carrier, they also market accounts widely and have winnowed their field of carriers down based on policy wording. Availability of higher limits also has an impact, but just "somewhat" for nearly 50% of respondents

For their part, underwriters' responses reflect that higher level of competition. Nearly 80% say retaining business on renewal over the last 6 months has become either much more challenging or a little more challenging.

As one broker put it, "This is a very crowded market. There are dozens of carriers offering coverage."

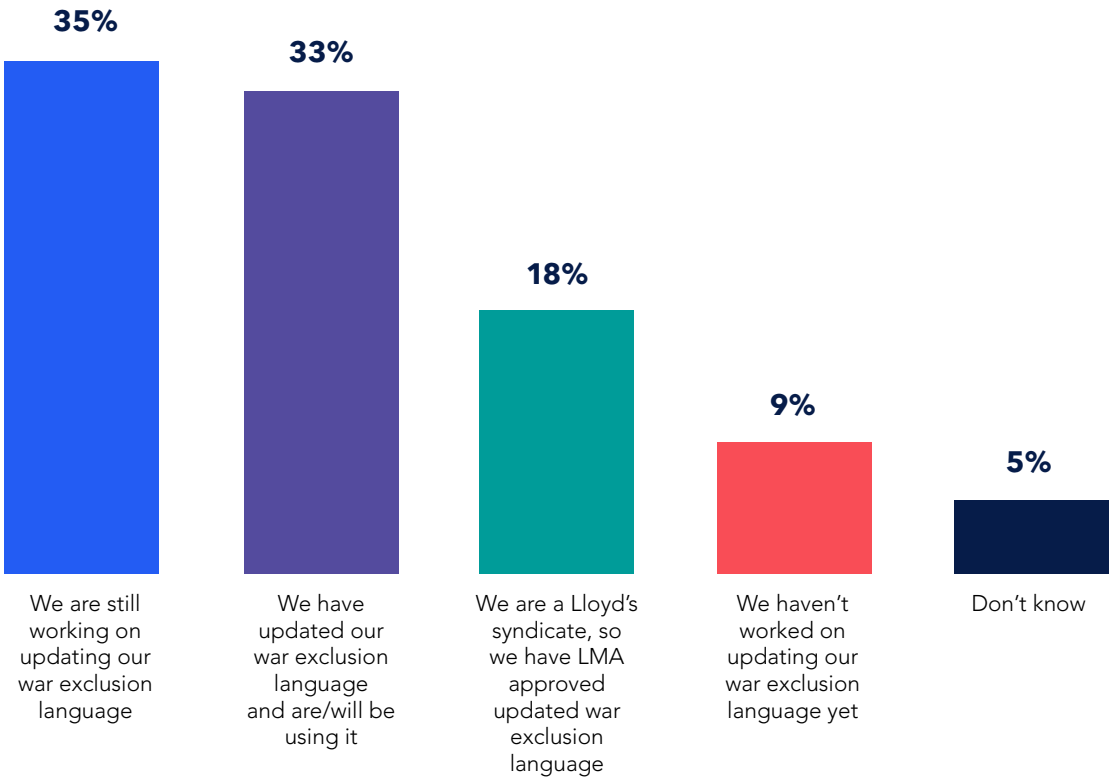
These results point to an "eye of the beholder" situation for the cyber market. One thing both sides agree upon – volatility in pricing and squabbles over coverage don't inspire confidence in buyers.

"Our target market does not share our enthusiasm for whacky coverage and an irregular pricing cycle," observed one respondent, and another noted, "too much yo-yo reaction to loss ratios. We need more stability."

War Over Words

After a yearslong process, the Lloyd's Market Association implemented a mandate for all Lloyd's syndicates to include modernized war exclusion language in their cyber policies. However, in practice, modernizing the war exclusion and getting market consensus has been a challenge, even though there are several efforts underway. In fact, only 9% of underwriter respondents note they have not worked on updating their war exclusion, while 33% responded that they have updated their exclusion and are/will be using it leaving a large swath of the market somewhere in between.

With efforts being made to modernize the war exclusion, where does your company stand?



Some brokers have also started developing their own war exclusion wording, although 63% don't expect to have their own language – and for the few that do, they are not requiring its use.

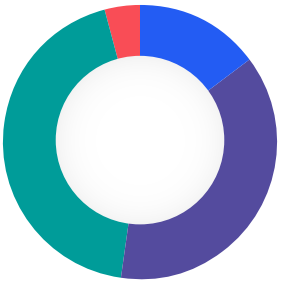
Despite the clear move toward updating language by much of the market, underwriters and brokers expressed frustration, particularly with the LMA's approach and end results.

One comment summarized the state of affairs on war exclusions for brokers: "We are well-versed in the concepts, but nobody understands all implications, especially with vague concepts and untested (in both claims and court) language such vas impacted states and major detrimental impact."

One of the hotly debated issues around the war exclusion is whether collateral/bystander asset damage (impacted entities outside the physical war zone), from state-sponsored cyberattacks should be covered. Again, there was divergence between brokers and underwriters, with only 11% of brokers responding they should not be covered, while 44% of underwriters felt they should not be covered. The difference could stem from understanding all the implications of the war exclusion as 49% of underwriters felt they were well-versed in all the complexities of the wording, while only 18% of the brokers felt the same way.

Do you feel collateral/bystander asset damage (impacted entities outside the physical war zone) from state-sponsored cyberattacks should be covered?

Underwriters



- **15%** Yes – fully
- **38%** Yes –to an extent
- **44%** No
- **4%** Don't know

Brokers

- **36%** Yes – fully
- **44%** Yes –to an extent
- **11%** No
- **10%** Don't know

Modernizing war exclusions has been disruptive to the market.

Nearly 60% of brokers say it "depends" whether they would move business to a different carrier based on war exclusion wording, which leaves a lot of uncertainty for carriers.

And 33% of underwriters noted lost business due to their modernized war exclusion, while 13% have seen more business because they don't have a modernized war exclusion.

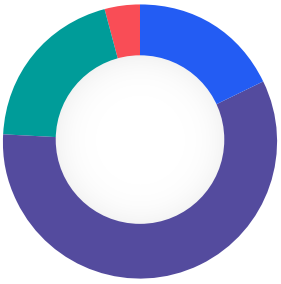
If you are using a modernized war exclusion, have you lost any business because of it?

Underwriters

- **6%** Yes – a lot
- **27%** Yes – some
- **25%** No difference
- **13%** Don't have a modernized war exclusion, but seeing more business because others do
- **15%** Don't have a modernized war exclusion, no impact on our business flow
- **13%** Don't know

With efforts being made to modernize the war exclusion, will you move business to a different carrier based on war exclusion wording?

Brokers



- **6%** Yes, it's a very important consideration for most of my clients
- **27%** Depends
- **25%** No, it's not that important to my clients
- **13%** Not applicable

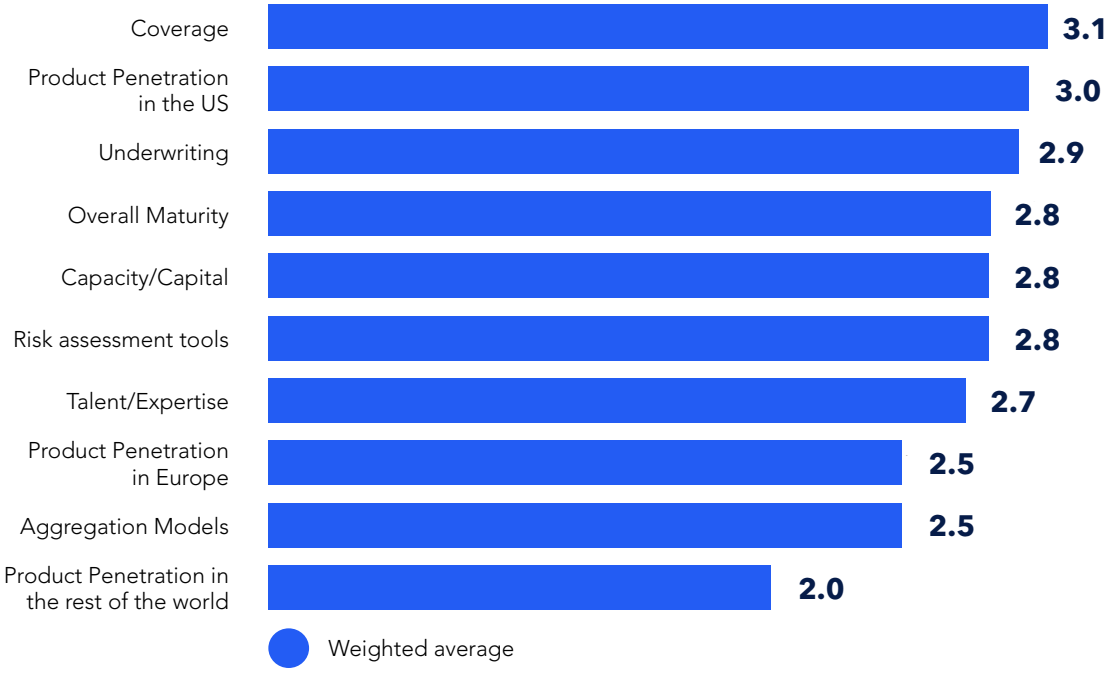
Market Maturity

According to respondents, the cyber market's overall maturity is at the halfway mark.

As one respondent noted, "In a world where the attack surface and strategies are constantly changing, it is hard to imagine reaching peak maturity."

Coverage is one area where respondents genuinely feel close to the mark on maturity, despite the common complaint we saw in the commentary that there needs to be "more consistency between carriers and coverage/exposure evaluations" and "more standardization of coverage language and data analysis and pricing of components." These comments are supported by the fact that over 80% of brokers are seeing wide variation in price and/or coverage.

From your perspective, has the cyber insurance market achieved maturity? Please rate each metric on a scale from 1 to 5, with 1 being not mature at all, and 5 being full maturity:

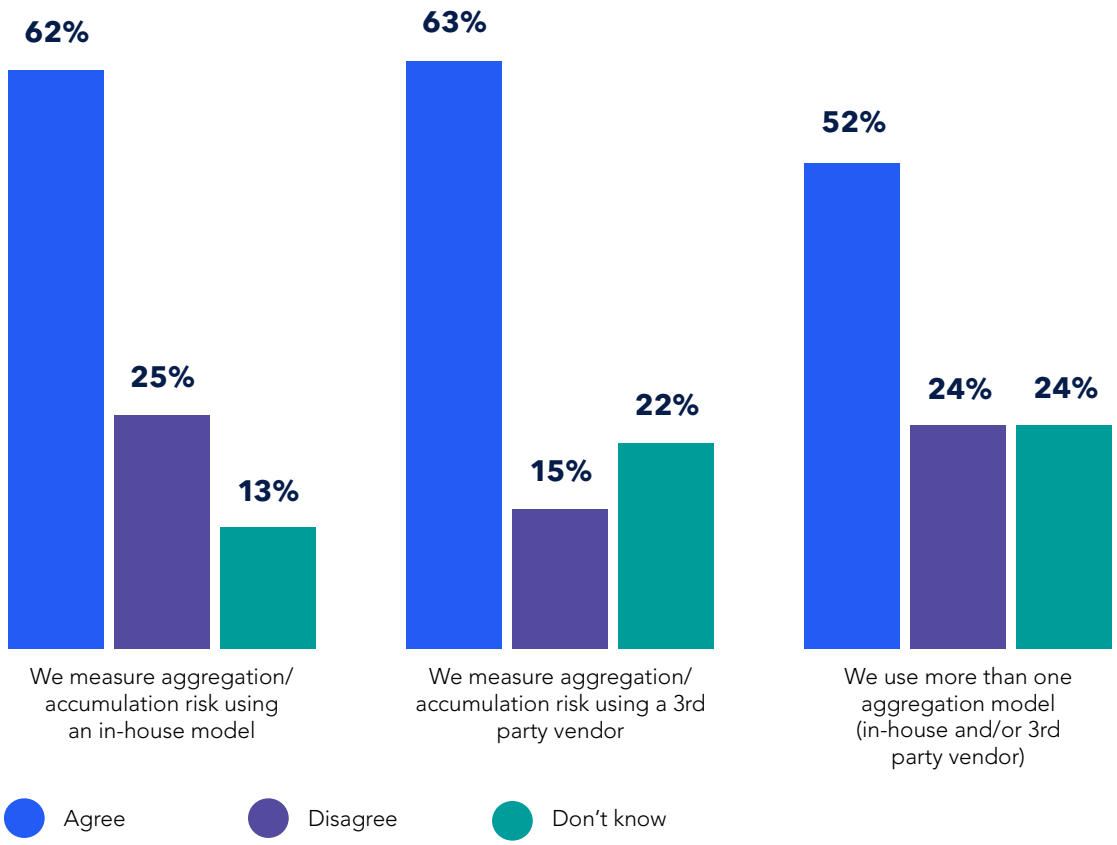


Over three-quarters (76%) of respondents indicated the market has become more sophisticated in the past two years, and in addition to coverage, the areas of greatest maturity were deemed to be underwriting, risk assessment tools, product penetration in the U.S., and capacity. The areas of least maturity were in the aggregation models, talent/expertise, and product penetration outside of the U.S.

Aggregation

Although respondents cited aggregation modeling as an area lagging in maturity, the survey results also indicate a significant level of attention is paid to accumulation risk. Over 62% of underwriter respondents said they use at least one model (either in-house or third party) to assess their aggregation and most use more than one model.

What do you predict for average rate change in the next 6 months?



Cyber Expertise Expands

Even though talent/expertise did not rank as high as some other elements on the maturity scale, respondents say the underwriters/brokers they work with are either "very experienced in cyber" (36%) or "knowledgeable in cyber, but not experts yet" (48%).

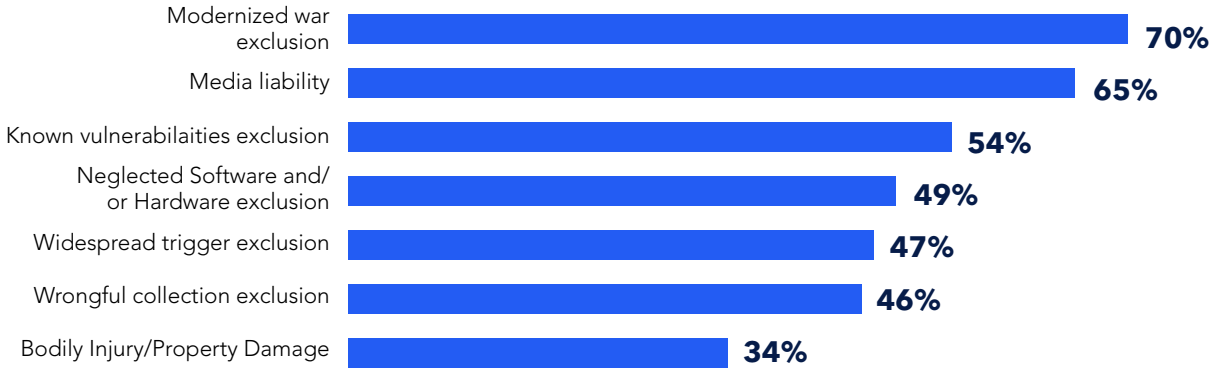
For a still-developing market, this represents a good track record – particularly when not so long ago, lack of expertise was a common complaint.

The cyber market draws from a deep bench of insurance experience, but cyber is still comparatively new for many of the professionals working in it. With so many professionals having come from other lines of insurance, they may be working from a playbook that functions well for traditional lines of insurance. Whether this strategy functions well long term for cyber remains to be seen.

The Future of the Cyber Policy

Looking toward the future of the cyber product, the underwriter responses hint at hopes to manage aggregation risk by having several exclusions part of a standard policy, such as the modernized war exclusion, wrongful collection exclusion, widespread trigger exclusion, known vulnerabilities exclusion, and a neglected software and hardware exclusion. Fewer broker respondents felt these exclusions would be standard in a future cyber policy.

What do you predict for average rate change in the next 6 months?



As one underwriter noted, "Cyber policies should provide cover for events we can predict and underwrite against, as well as manage from an aggregation perspective. Fringe covers that are typically thrown in without any thought have potential to destabilize the entire product."

But brokers and underwriters disagree on what those "fringe covers" might be.

'Very Short Memories'

The market has clearly shifted quickly once again, despite the growing concerns over rate adequacy, rising losses, increased third party privacy litigation, and coverages.

One respondent had some advice for market players. "Carriers need to take longer term views and not race to the broadest coverage/largest limits. Brokers also have a role to play as they need to learn from the last couple of years when carriers reduced line sizes, leaving clients with fewer options, but now want to increase line size again. There seem to be very short memories," they said.

Others cited some market players "driving poor decision making" with little regard for long-tail cyber claims or developing third-party liability.

The cyber market's strengths can also be its weaknesses if not managed skillfully. The ability to see losses in action, to leverage threat intelligence on a continuous basis, to tweak pricing quickly, and require high levels of cyber hygiene of insureds – these can serve to keep underwriters on pace with the exposures. They may also keep the market continually reacting to the "now" rather than thinking toward the future.

Long-term success and market maturity will hinge upon industry players' ability to demonstrate confidence in their pricing, underwriting, and portfolio management.

We are happy to make the results of the survey available to you. For survey results, or any questions or comments regarding this whitepaper, please reach out to **Catherine Rudow**, Global Head of Cyber Reinsurance, at catherine.rudow@everestglobal.com.

We fielded responses from 270 cyber professionals - 30% underwriters, 40% brokers, and 7% incident response. The majority are US-based and so are their clients. Respondents selected insureds with less than $250 million in revenue as their most common clients, though all levels of revenue were represented.

Primary standalone is written/placed by nearly all respondents, but brokers and under-writers still offer blended policies and endorsements.