2024 US MARKET OUTLOOK SERIES

RPS RISK PLACEMENT SERVICES

CYBER

Executive Summary

Cyber insurance is a market experiencing volatility, both in terms of the risks it faces and the premiums it offers to clients.

This volatility makes it a difficult market for agents to operate in – a fast moving threat landscape, ever changing client needs, and constantly rising and falling premiums make expert advice a must.

Whether it's better understanding which cyber controls are needed to access the best levels of cover, determining the cause-and-effect of policy wordings, or establishing where the market is heading next, wholesalers like RPS are valuable partners to any agent looking to increase their sales of cyber insurance.

The latest Cyber Outlook Report from RPS discusses how a worsening claims landscape, coupled with a year-plus of softening rates, could set the table for a relatively short-lived soft market.

Cyber insurance is very different from the wider P&C market, and at no time has that been more apparent than in the current landscape.

The cyber market has seen rapid growth in recent years, but during that time, the cycle between hard and soft markets has been quick and volatile – much more compressed than the slowly evolving cycles experienced across other insurance lines.

This is largely due to the constantly changing threat landscape presented by cyber perils themselves, and Risk Placement Services (RPS) National Cyber Practice Leader Steve Robinson says this volatility makes it a particularly challenging market to navigate.

"The perils facing cyber insurers are constantly changing in ways that cannot be predicted, and that means the market has to adapt quickly," he says.

Robinson cites the wave of innovation between 2014 to 2019 that saw extended coverages and falling rates as a great example of a developing market, but this was soon followed by a period of intense hardening and maturity between 2020 to 2022 as ransomware became the more pervasive threat.

During this time rates rose quickly, sometimes reaching triple-digit increases, and up until late 2022 the market continued to harden. RPS Area Vice President Dillon Behr says that these challenging conditions were compounded by a perceived "overcorrection" from insurers.

"We saw some drastic price increases over this period on the heels of lots of ransomware claims from 2018 to 2021 that took a year or so to hit the books," he says. "Insurers then had to work through a whole cycle of increasing rates and tightening controls and, before you know it, claims are dipping and insurers start to get comfortable again because of the high premiums they had been charging."

This led to the market turning again as we moved into 2023, with markets quickly thinking they were "out of the woods" as ransomware events fell and premiums followed suit, with the cycle continuing at pace even if the data didn't back it up.

3

"Insurers started taking rates back down with less than a year of favorable claims data," Robinson says. "A lot of that was newer players that were accustomed to huge revenue from rocketing rates and higher policy take up."

"Investors that had backed some newer players in 2019–2022 were asking why their investments were not growing as fast anymore, and markets responded by reducing rates to capture market share – but that was counter to everything the market knew over the last three years."

RPS Area Senior Vice President Nick Carozza says insurers have also been expanding their appetite and increasing limits in order to offer more appealing coverages to insureds.

"We're not quite at the point where insurers are offering terms like they did pre-2020, but there are carriers who are getting a lot more aggressive in offering higher limits and being a lot more relaxed in the types of controls they are asking for from their insureds," he says.

RPS Area Assistant Vice President Kunal Mallik agrees, and says that higher limits are an increasingly common theme across the cyber market.

"A couple of years ago, getting a $10 million limit was almost unheard of," he says. "Most insurers were offering a maximum of only $5 million in limits, but now you have insurers who, depending on the nature of operations and the class and the size, might be willing to offer $10 million, so there's more capacity available."

Several insurers have also reduced their multi-factor authentication (MFA) and endpoint detection & response (EDR) requirements, even across higher revenue bands.

This means that 2023 was very much a buyers' market, but with claims already rising again, the current trends will not be sustainable over the mid to long-term, and agents must prepare themselves once again for stabilization, even rate increases.

This environment is a sort of "purgatory" for agents, even if the current market makes it easier to do business, and RPS predicts that these favorable conditions for customers are not going to last.

And Mallik says that the reason why the cyber market hasn't already hardened is, in part, because of the increased competition as a result of new entrants.

"Insurers have also been expanding their appetite and increasing limits in order to offer more appealing coverages to insureds.

"We're at a period where a correction is likely," he says. "So far that's been offset by the amount of new entrants coming into the marketplace providing additional capacity, and that increased competition has stalled some existing insurers from readjusting their pricing.

"But that's likely only going to be sustainable for the next quarter or two, and when those pricing adjustments do hit, while they might not mirror the drastic increases we saw a couple of years ago, they could be substantial for some."

He adds, "The current pricing model just isn't sustainable at all – a market correction on pricing is overdue."

Carozza agrees, and says the same market dynamics that pushed new entrants to reduce premiums, could now lead to them pushing up rates in the near future.

"A lot of the new carriers we saw entering the market were buying market share by lowering their premiums, which has been causing significant disrupt," he says.

"But what happens when you're not as profitable as you hoped you would be? You have to increase premiums, and pull various underwriting levers to return to a more profitable position."

Some sectors will be harder hit than others, with manufacturers and other industries exposed to a high risk from business interruption and expected to face more significant price increases.

"These classes of business tend to have the highest claims payouts because of the high levels of business income exposure," Carozza says.

"Their high reliance on system uptime in order to make their products makes them a prime target for ransomware attacks. As a result, this remains an industry we're seeing top the list for claims frequency."

And this could lead to challenges in placing risks for insureds in these industries.

"The most challenging sectors for coverage placement, particularly among larger risks, are manufacturing, contractors, municipalities, and anything in the financial services sector," Carozza says. "We're seeing a lot of rate being left on those already, and carriers are expecting controls to be really tight as well."

Another reason for cyber's anticipated return to a changing market is a worsening claims landscape that is reflective of new threats and the return to prominence of some familiar ones too.

"The current claims trends are not correlating with the rate decreases we've been seeing, nor the lower barriers to entry from some insurers, and that is a very counterintuitive position to be in," he says. "Claims experienced by many insurers have hit pre-2021 frequency, but some markets are in a race to the bottom, and we are all just waiting for the ball to drop."

Mullen Coughlin, LLC, the leading US cyber incident response law firm, offers an interesting view of reported cyber matter trends, as their extensive data is representative of a wide swath of organization sizes and industry sectors. The firm's 2023 incident response data substantiates reports of a far more active threat landscape. Through November 2023, business Email Compromise incidents accounted for a 35% increase in frequency over 2022, eclipsing the previous annual highs experienced back in 2021. Following closely at a year-over-year increase of 22%, across all industries, was ransomware.

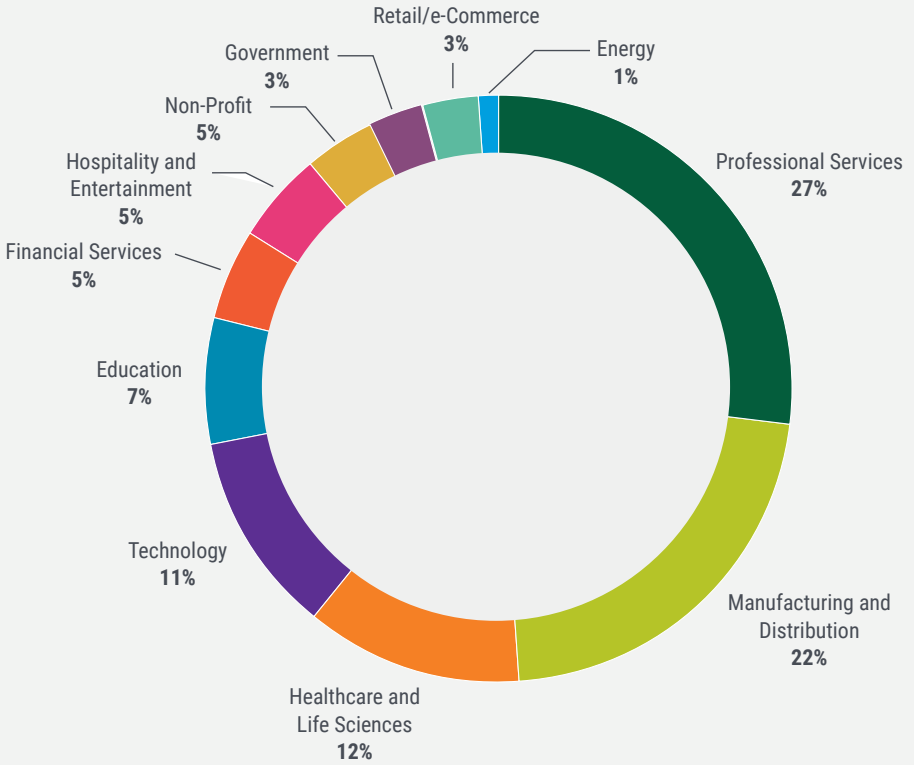
2023 INCIDENT RESPONSE DATA

INCIDENT TYPE	COUNT>2022
Business Email Compromise (BEC)–Total	35%
Ransomware	22%
Third-Party Breach	19%
Other	10%
Network Intrusion	8%
Inadvertent Disclosure	6%

Source: Mullen Coughlin, LLC

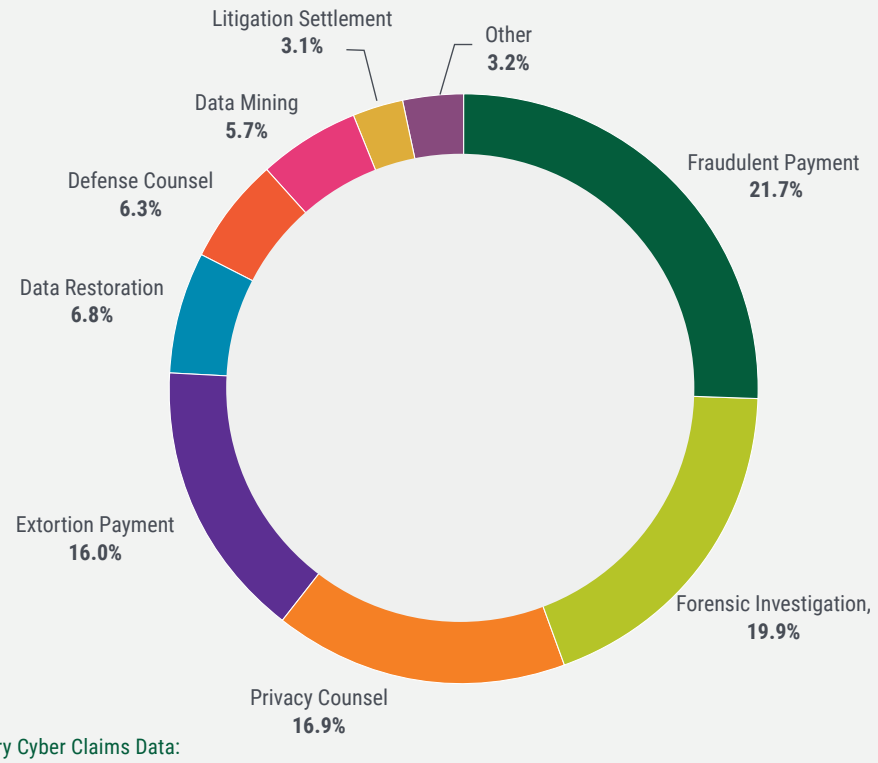
The Mullen Coughlin 2023 claims data also shows that industries leading the way in ransomware activity were Professional Services (27% increase in frequency over 2022), Manufacturing and Distribution (22% increase), Healthcare and Life Sciences (12%), Technology (11% increase), and Education (7% increase). Financial Services, Hospitality and Entertainment, Non-Profit, Government, Retail/e-Commerce, and Energy all experienced increases in ransomware frequency over 2022. This data further underscores the dichotomy that is occurring in the cyber insurance pricing world and how it is often not reflective of current claims trends.

INDUSTRIES LEADING IN RANSOMWARE ACTIVITY



Source: Mullen Coughlin, LLC

PERCENTAGE OF CLAIMS DOLLARS PAID - SME INSUREDS



Source: 2023 RPS Proprietary Cyber Claims Data: Insureds < $100M Annual Revenue

While fraudulent payments accounted for the most dollars paid out among RPS small business insureds in 2023, it was due to a significantly higher frequency rate than ransomware events. However, ransomware continues to have an outsized impact on organizational disrupt and insurer profitability. While ransomware accounted for only 13% of reported matters in 2023, the impact of a ransomware event can be felt across many categories of claims payouts as demonstrated in the percentages of RPS small and medium-sized insured (SME) paid claims above.

Behr says that in order to effectively manage the volatility created by these constantly shifting sands, agents must be smart in how they present solutions to their clients.

"Cyber has never been about getting the cheapest product available, but in this changing market, finding the right product is more important than ever," he says. "Agents need to make clear to their clients that the low premiums being offered today likely won't be the same at the next renewal; it's just not sustainable, and they need to be prepared for that.

"Agents should use this as an opportunity to enhance coverage based on a thorough review of the business needs of the company, using the budgets available to purchase cover at a higher level. Then, when prices go up next year, there is always the option of reducing coverage but still being able to afford adequate cover."

The team at RPS also cites the significant increases in other coverage lines, such as Property as recipients of premium re-distribution as cyber rates have fallen. Robinson adds, "While insureds should view these temporary savings as an opportunity to right-size their cyber limits, some have deployed those cost savings to other areas of their insurance program that are experiencing significant increases." It is always easier to renew at higher limits than it is to source higher limits for the first time as the market changes, and capacity inevitably tightens once again.

YOU GET WHAT YOU PAY FOR

In insurance, the mantra you get what you pay for is a common one. But this is especially true when it comes to cyber insurance.

Mallik says this is because cyber coverage is more of a partnership than many other P&C business lines.

"You want to partner with a market that not only understands cyber and has significant experience in the space but one that is actively putting resources into understanding the space better five or even 10 years down the line," he says. "This will put your clients in a much better position than if you just select a policy based solely on price, and end up with someone who has just entered the market but might be exiting again after two or three years of not pricing things appropriately."

This is because those insurers that are thinking about the cyber market with a longer term perspective will have been able to invest more heavily in their support services.

"These insurers are bolstering their internal software and teams to provide resources to their clients to prevent attacks from being successful, rather than just paying out claims after the attacks occur," Mallik says.

Most established insurers often offer a swathe of additional services too, including things like anti-phishing tests, and it is the agent's job to encourage their clients to use them to help mitigate the risks facing their business.

"One of my biggest issues is that only 8%-10% of insureds are using these additional services, and I am talking to my agents about encouraging their clients to take their insurers up on using these services," Carozza says. "The industry as a whole needs to do a better job of making it known to the buyer that they have these additional risk management resources available to them as a policyholder."

> "One of my biggest issues is that only **8%-10%** of insureds are using the additional protection services offered to prevent a cyber attack.

The issue, however, is that there is often not enough time given to discussions around cyber cover.

"The problem with cyber being an ancillary product for many is that it is often the last thing that's discussed at a renewal meeting," Carozza says. "And while it is usually among the smallest premium in their insurance program, this line of coverage is experiencing an increasing frequency of incidents."

"So agents need to sit down with their insureds and make sure they are giving cyber applications the time they need, and not just answering yes or no to questions without fully understanding the ramifications."

But Mallik says the current market conditions can help to bring cyber insurance to the fore.

"The reason cyber is still seen as an ancillary product is because many insureds just don't think they are at risk of attack," he says. "So there is a lot of education that needs to be carried out to demonstrate to buyers the very real risks they are facing and the benefits of having cyber coverage in place.

"The good news is that there is still a lot of capacity out there, and coverage is relatively easy to come by, so it is a great time to be exploring the benefits of a cyber policy with your clients."

And it is here that wholesalers like RPS can help.

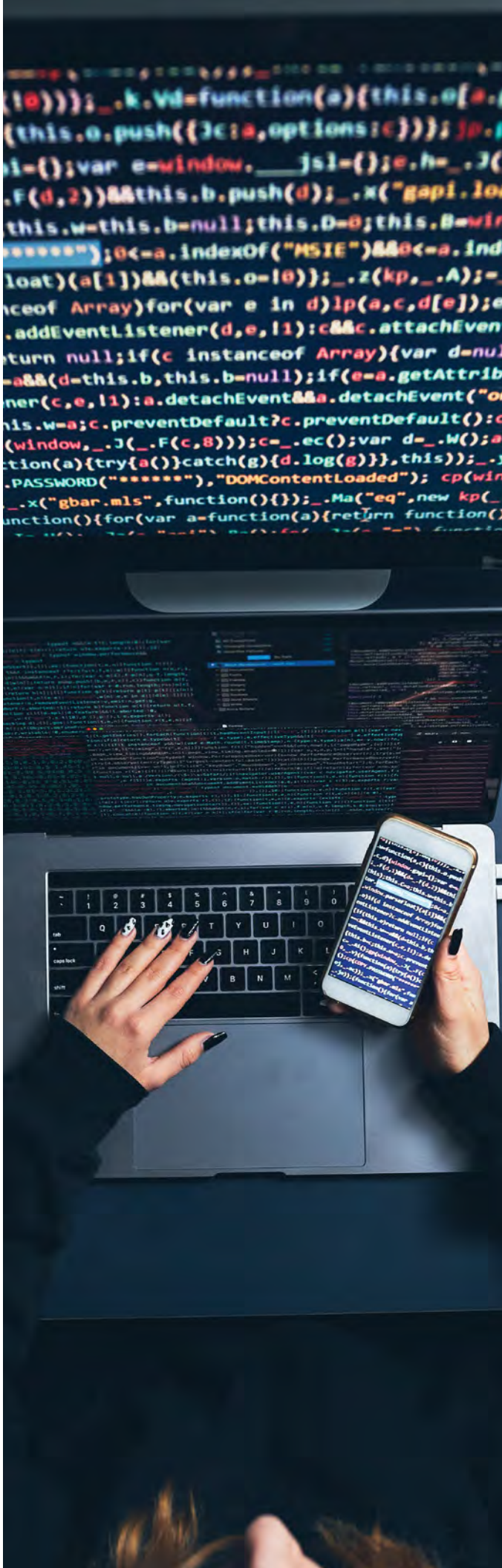
"Agents can gain a lot by partnering with the right wholesaler, whether that be comparing different quote options line-by-line, or getting into the detail of policy form wording and explaining what is and isn't covered and any implications that might have on a claim," Behr says.

"We want to be an extension of our agents' placement team, and I would encourage anyone working in cyber to really lean into these partnerships and to bring their wholesalers to the forefront of any discussions they are having about cyber coverage."

THE POWER OF CONTROL(S)

Insurance and controls have always gone hand-in-hand in the cyber market, working together to help mitigate and protect against the risks being presented by hackers and other threat actors.

And insurers for a long time saw control processes as a necessary requirement for insureds looking to access higher levels of cover, but shifting market dynamics are changing that for some.



"Some carriers are being a little bit more flexible now, particularly for small business," Mallik says. "A year or two ago, if you didn't have multi-factor authentication (MFA), you almost always found yourself in a situation where you weren't going to get full ransomware extortion coverage, or, if you did, there would be a limitation either via co-insurance or a smaller sub-limit for cyber extortion.

"But due to the competitive landscape, some carriers are now more willing to offer those limits at full capacity with a lower level of controls in place, just because they have to stay in the market and avoid losing business to new entrants that may not be as strict on their requirements."

The rise of generative A.I. however, may change things again.

"Generative AI is certainly a looming threat for the cyber market," Mallik says. "We've seen hints of this already with ChatGPT and just the sheer capabilities of smart tech. We have to be wary of this, because it gives the threat actors significantly expanded capabilities, and this is very concerning for the industry.

"As these threat actors are increasingly able to use generative AI to create malware that not only adapts but also responds to defenses, the landscape continues to change. Because then you're in a situation where malware would be able to evade, change, and transform, and ultimately becomes increasingly difficult to take down."

And these hackers are already using new tools and techniques to get around controls that, historically, have been excellent gatekeepers.

"MFA bombing, or MFA fatigue attacks, is a new attack vector that we've been seeing more of lately," Mallik says. "It's when someone uses social engineering or phishing to gain your initial credentials, and then they're able to spam you and get you to react to your second form of verification of identity to gain access to your systems."

So while MFA may have historically protected organizations from the majority of ransomware attacks, no longer is this always the case, and security requirements could be about to change again, with Mallik predicting a future increase in the levels of identity verification needed in order to make a system secure.

"Dual authentication can certainly be less effective as a result of this MFA bombing," he says, "and we are going to have to jump to the next level. But the question is: where does this all stop? Are we just going to keep needing verification on top of verification?"

"Dual authentication can certainly be less effective as a result of this MFA bombing, and we are going to have to jump to the next level.

> **Agents who maybe aren't fully versed in cyber, if they aren't used to selling it day in, day out, need to make sure they partner with someone who has extensive experience in the market.**

And Behr says deep-dive policy analysis services such as these have become particularly important of late, with it becoming increasingly difficult to differentiate between coverages – especially for non-experts in the field of cyber.

"You might be able to tell if it covers extortion, or if it covers things like business interruption or social engineering, but do you understand the nuances of those coverages and the limits associated with them?

"Agents who maybe aren't fully versed in cyber, if they aren't used to selling it day in, day out, need to make sure they partner with someone who has extensive experience in the market, someone who really specializes in providing cyber cover, and really understands the trends."

Mallik says that the current market dynamics also mean it has become more important for brokers to go out to market and see what is available when placing a risk.

"The appetite of insurers is changing weekly," he says. "This means agents need to put these risks out into the market, not just to see what prices are available but to see what is available in terms of coverage too."

"That also has the benefit of allowing you to leverage your position," he adds. "There is, of course, an importance in business continuity and having long-term partnerships with carriers. But there is also importance in realizing what's out there, and how things are changing and how they can be an advantage for you and getting your client the coverage that they need."

For Robinson, the situation is clear.

"You can't have someone with static expertise advising on a dynamic risk like cyber," he says. "That's where you need a partner like RPS to give you the advice and guidance needed to deliver the best for your clients."

About Risk Placement Services

Risk Placement Services (RPS) is one of the nation's largest specialty insurance products distributors, offering solutions to independent agents and brokers in wholesale brokerage, binding authority, programs, standard lines and nonstandard auto. The RPS team, fueled by a culture of teamwork, creativity and responsiveness, works with top-rated admitted and nonadmitted carriers to design robust coverage for clients through its more than 80 branch offices nationwide.

For more information, visit RPSins.com.

CONTRIBUTORS

Steve Robinson, National Cyber Practice Leader

Nick Carozza, Area Senior Vice President

Dillon Behr, Area Vice President

Kunal Mallik, Area Assistant Vice President

RPS RISK PLACEMENT SERVICES

RPSins.com

RPSUS45581 0124