WOODRUFF SAWYER

Looking Ahead

Cyber Insurance Trends for 2024

Get Started →

Table of Contents

1.0

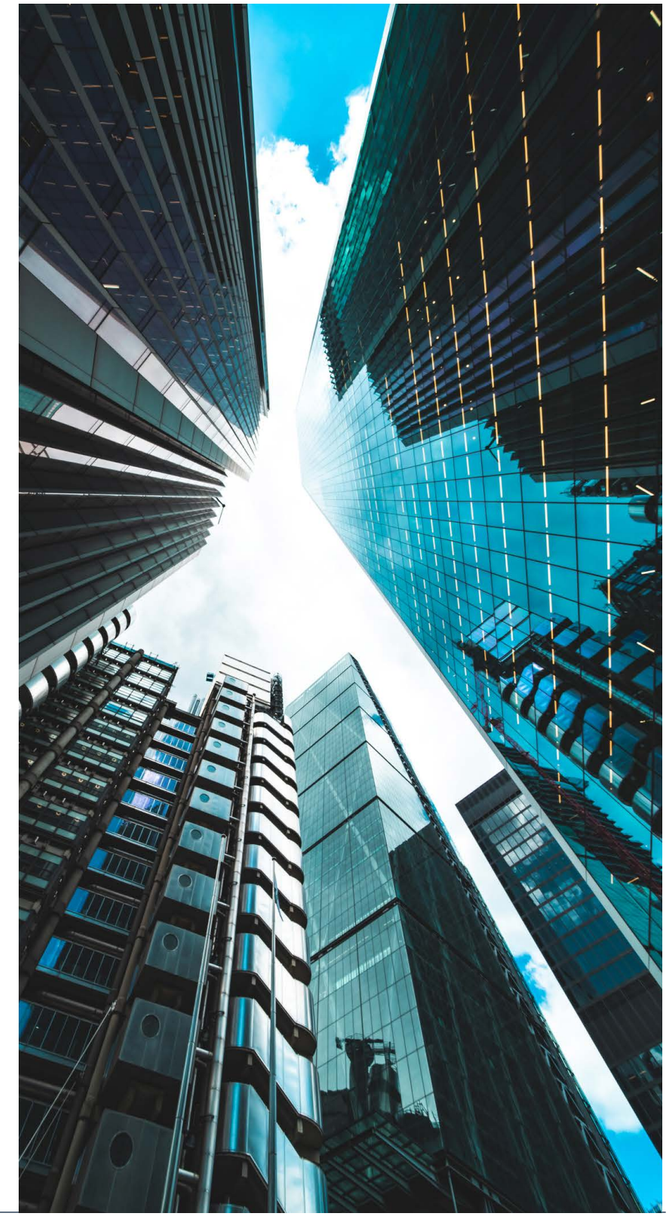
Cyber Market Update

Start >>

Dan Burke
Senior Vice President, National Cyber Practice Leader
415.402.6514 | dburke@woodruffsawyer.com
View Bio
LinkedIn

1.1 US Market Update

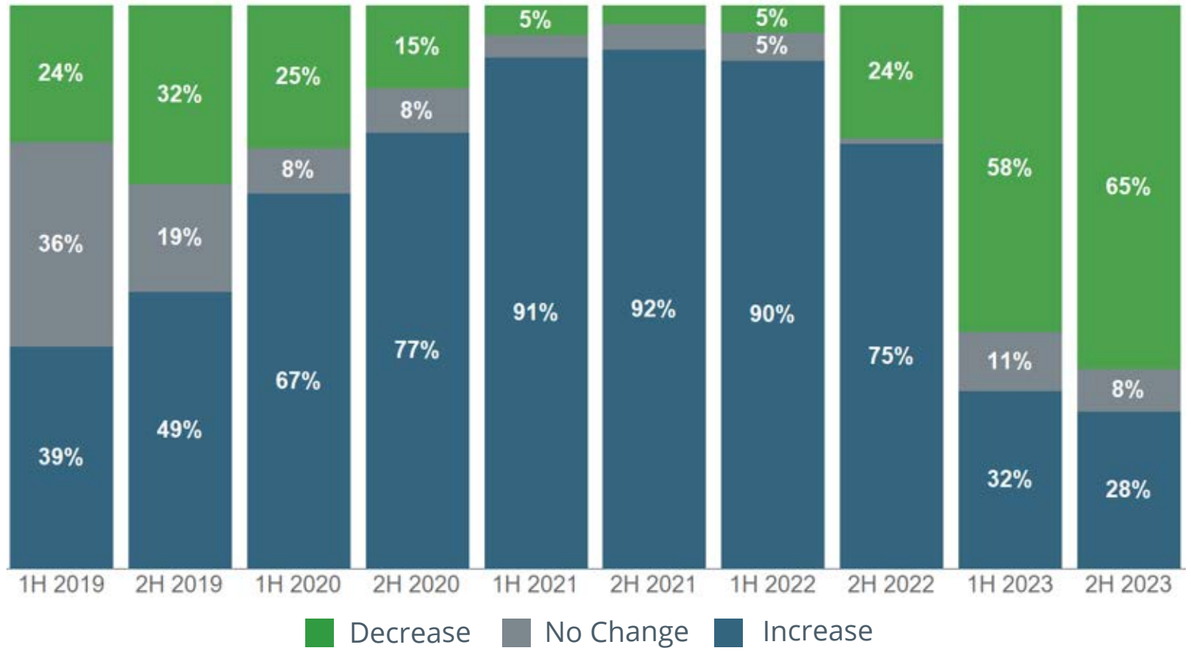
Followers of the cyber insurance market over the past two years may be suffering from whiplash—that's how dramatically the market shifted from 2022 to 2023. A perfect storm of good trends and facts combined to create a soft cyber insurance market—still-elevated after a two-year hard market, reduced claim experience due to a lull in ransomware throughout 2022, and improved cybersecurity controls at the insured company level driven by insurance underwriting mandates. Many of Woodruff Sawyer's cyber insurance clients saw decreases in the cost of their insurance throughout 2023—58% of clients in the first half of the year and 65% in the second half.



US Market Update (cont.)

65% of Our Clients Experienced Cost Reduction in 2H 2023

Cost Change in Cyber Insurance Renewals Over Last 4 Years



Source: Woodruff Sawyer Program Renewal Analysis

Notes: Data shows percentage of clients who experienced flat or change in renewal premiums for their cyber program and does not indicate percentage premium increase or decrease. 2H 2023 is based on data through 12/8/2023. Percentages may not total 100 due to rounding.

Here are some of the key insurance market themes that emerged throughout the year.

The War Exclusion Enters the Chat

No coverage issue was more front and center in 2023 than the war exclusion. Many carriers launched revised language this past year—spurred by a mandate from Lloyd's of London to its syndicates. Initially intended as a clarification of coverage, the revised approach to war exclusion language was anything but clear. The "fog of war" apparently also applies to insurance language.

Expect this to continue playing out in 2024, with carriers trying to clarify how their cyber insurance policies treat nation-state-backed attacks against the private sector.

Roadmap for Plaintiffs or Boon for Investors: The SEC's New Cyber Rules

The Securities and Exchange Commission's new cyber disclosure rules are here. Review the big-picture items you need to know.

Ransomware Is Back—Same as It Ever Was

Carriers started sounding the alarm as early as the second quarter of 2023, and by the end of the year, the trend was clear—ransom claims had risen to 2021 levels, the highest year of ransom claims on record. And while a smaller share of companies paid the ransoms demanded, these payments were dramatically higher.

We also saw an increase in attacks that relied on data exfiltration (also known as data theft) as opposed to the deployment of network-encrypting malware. Attackers are exploiting a reality that many companies have discovered: Data is often most valuable to the company from which it is stolen. The threat of disclosure of being hacked is sometimes enough to make a company pay a ransom. But that calculus may be changing in 2024—driven by the Securities and Exchange Commission's (SEC) disclosure requirements.

Coverage Restrictions for Systemic Risk and Privacy Violations

The underwriter survey in our *Looking Ahead Guide to 2023* predicted a coverage retraction in the cyber insurance market—and the underwriters delivered. In addition to the confusing war exclusion changes, we saw carriers add complicated restrictions for systemic risk. We also saw carriers react to pixel tracking claims and privacy concerns by restricting coverage for wrongful collection—the collection, processing, storage, or use of data without proper consent from consumers. These pixel tracking claims were concentrated in the healthcare space in 2023 but expect more activity outside healthcare in 2024.

Client Cybersecurity Maturity Brings More Suitors

The hard market of 2021 and 2022 ushered in an era of strict underwriting standards focused on specific cybersecurity controls. While this focus on cybersecurity controls has not waned, we see client investments in maturing their cybersecurity controls starting to pay off on the insurance side. Stronger cybersecurity controls strongly correlate to more carriers willing to offer insurance—creating the needed competition to drive premium savings.

Privacy Violations: Mitigation Strategies and Cyber Insurance Considerations

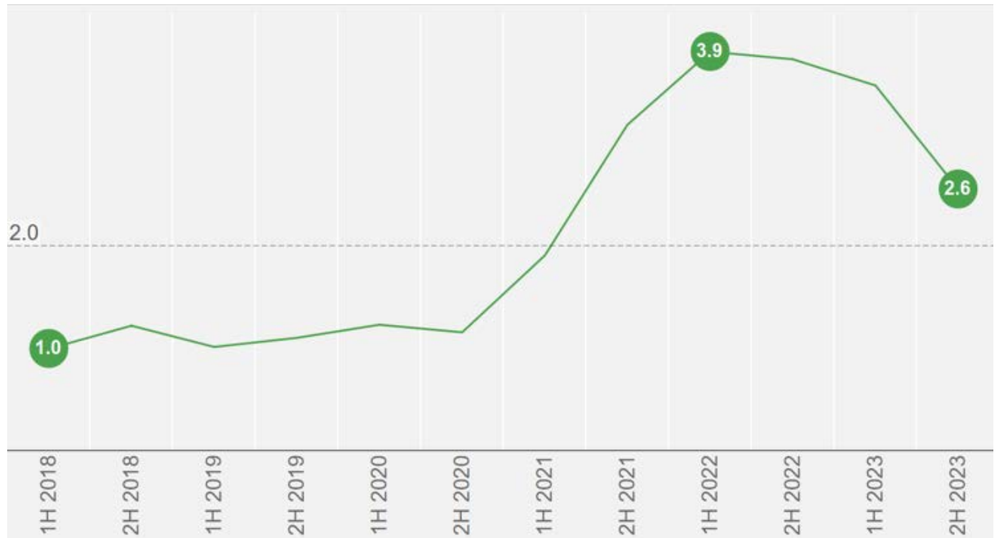
We've seen a surge in litigation involving privacy violations. Explore recent litigation and learn ways to protect your company from similar lawsuits.

1.2 Cyber Pricing Trends

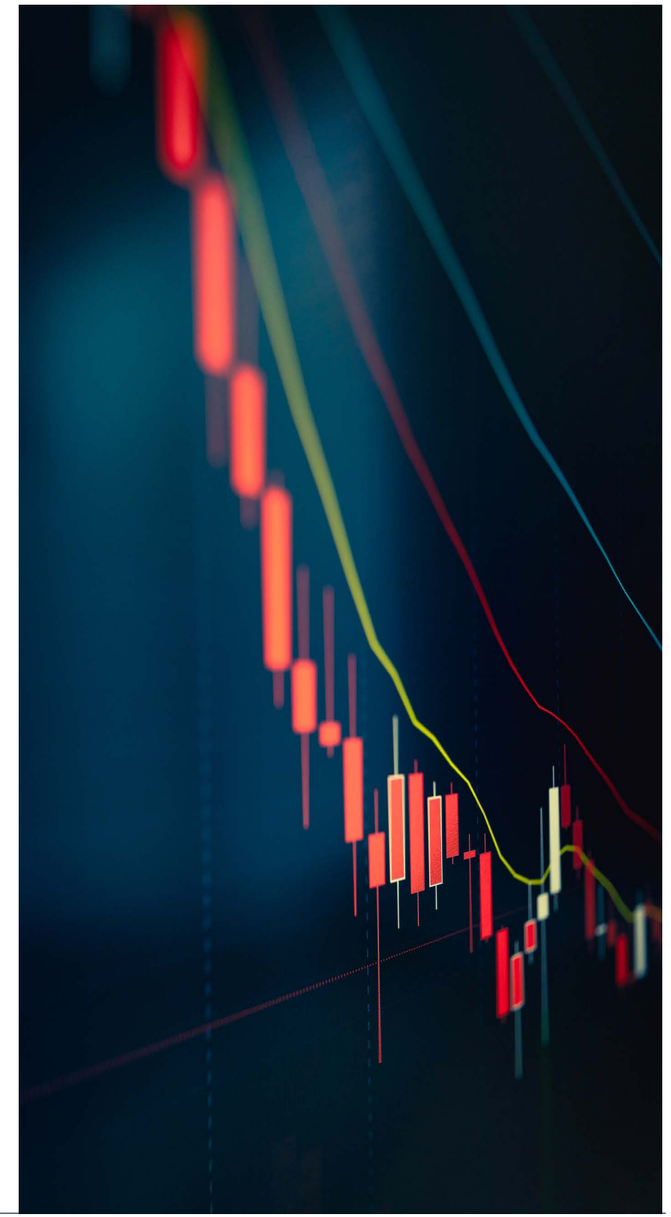
Despite many of our clients seeing total cost decreases, the cyber pricing environment remains elevated from pre-pandemic levels. The good news is that the hard market peaked in the first half of 2022. However, the rate decreases seen throughout 2023 have only brought rates in line with 2021 as opposed to the lower rates of 2018–2020.

Despite Rate Decreases, Premiums Are Still Higher Than In Recent Years

Cyber Insurance Market Rate Index (2018:Q1 = 1.0)



Source: Woodruff Sawyer Annual Clients Renewals
Note: 2H 2023 is based on data through 12/08/2023.



Cyber Pricing Trends (cont.)

Insurance carriers have pointed to statistics on ransomware activity reverting to 2019 levels to argue current pricing is unsustainable—but the median pricing level remains nearly three times higher than in 2019. This suggests that while rates may level off soon, carriers should not react as dramatically to the increase in ransomware activity. Said more bluntly: carriers have more premium on the books to negate this rise in claims costs and a dramatic increase in rates like we saw in 2021 and 2022.

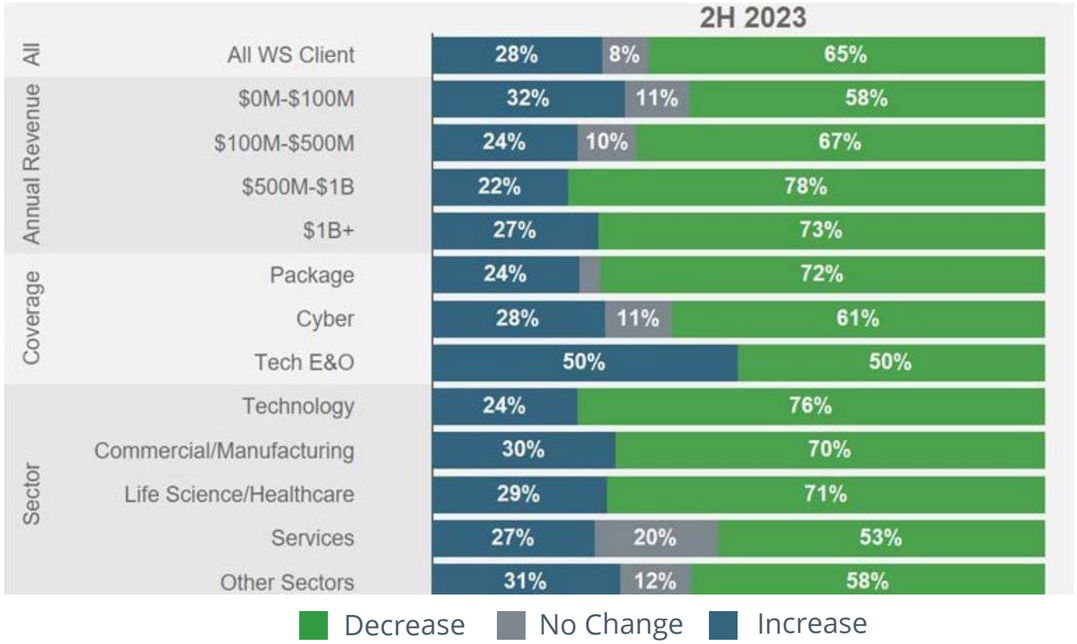
Technology E&O Pricing Trends

Looking at a specific segment of our cyber portfolio—technology companies that purchase a package policy of errors and omissions (E&O) coverage bundled with cyber insurance—paints a similar picture. The technology market was more constrained as 2023 kicked off, with limited capacity compared to the broader cyber market.

However, favorable legal rulings preserving Section 230 of the Communications Decency Act served to take some uncertainty out of the future liability risk for technology companies. As capacity in the market increased, we did see rates begin to fall and clients realize cost savings in their insurance programs.

A Majority of Segments Saw Insurance Cost Reduction

Cyber Annual Cost Change by Business Segment in 2H 2023



Source: Woodruff Sawyer Program Renewal Analysis

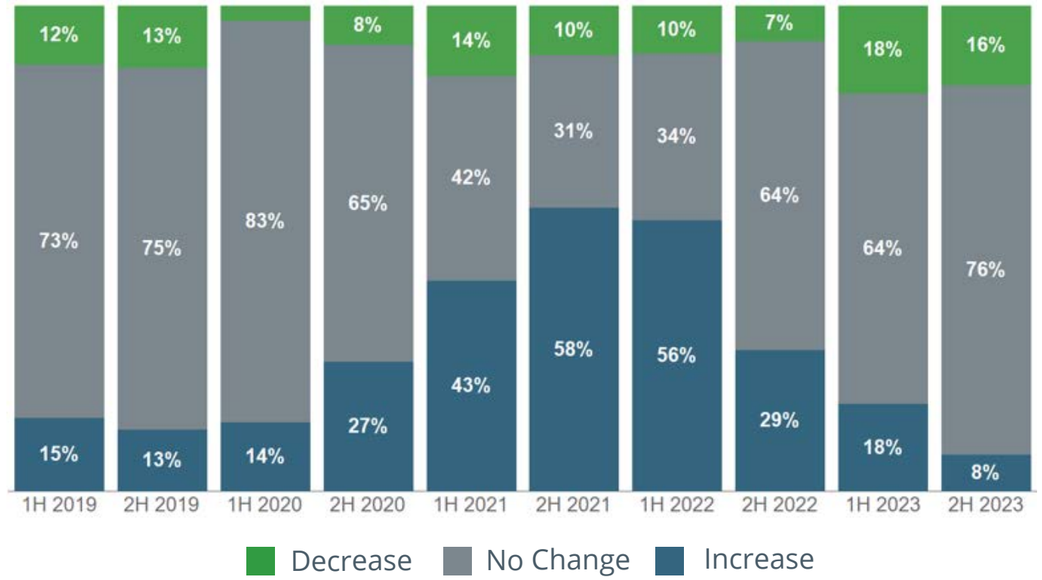
Notes: Data shows percentage of clients who experienced flat or change in renewal premiums for their cyber program and does not indicate percentage premium increase or decrease. 2H 2023 is based on data through 12/8/2023. Percentages may not total 100 due to rounding.

1.3 Self-Insured Retention Trends

The good news about the soft market ends when it comes to self-insured retentions (SIRs). While retentions increased during the hard market of 2021 and 2022, we have yet to see them begin to come down dramatically. Most of our clients (76%) have seen no change to their self-insured retention in 2023—suggesting that increases from 2021 and early 2022 were a true reset of the market as opposed to a cyclical or temporary increase. Higher retentions appear here to stay.

Most Clients Have Experienced No Change in Self-Insured Retentions

Cyber Insurance Renewals: Changes in Retention Over Last 4 Years



Source: Woodruff Sawyer Program Renewal Analysis

Notes: Data shows percentage of clients who experienced flat or change in retention and does not indicate percentage retention increase or decrease. 2H 2023 is based on data through 12/8/2023. Percentages may not total 100 due to rounding.

2.0

Hot Topics

Cyber risk is continually cited as a top concern for executives and board directors, and rightfully so. The digital transformation that is underway in every industry has led to increased cyber risk. Let's dive into some of the most pressing cyber risks companies face today.

Start >>

2.1 Cyber Warfare

Wars have consequences. This tried-and-true trope also applies to cyber insurance and the reality of modern warfare—cyberattacks are part of a nation-state's offensive arsenal. As mentioned earlier, cyber insurance carriers attempted to clarify their stance on cyber war and the application of the war exclusion in 2023—to little success. But they're not done trying.

> The current wars in Ukraine and Gaza bring the prospect of an attack spilling outside of intended targets and impacting the broader private sector into real focus.

After all, we've seen this scenario play out previously with the 2017 NotPetya attack.

This presents a systemic risk dilemma for cyber insurance carriers—should the cyber insurance market bear responsibility for supporting the recovery from the effects of a war?

This is where calls for a public-private partnership between government and the insurance sector are the loudest. We expect more momentum to build for such a partnership throughout 2024—if not the framework for a true partnership.

Nation-State Cyber Attacks and Insurance Response: Revisiting the War Exclusion

Read more to understand what the war exclusion means for cyber insurance policyholders, as well as how the potential inclusion of ransomware cybercrime groups in the federal sanctions list affects ransom payments.

2.2 SEC Cyber Regulations

Regulators have been pining to do what they love when it comes to cybersecurity—regulate it. The Securities and Exchange Commission (SEC) may be the most aggressive with its approach. The rules around disclosure of cybersecurity incidents for public companies have been well documented—and the requirement to disclose material incidents within four days of discovery will be a dramatic shift for those required to comply.

> The short time frame for determining materiality will likely have an impact on companies deciding whether to pay a ransom.

On one hand, the threat of public humiliation is dissipated when companies must disclose the incident anyway. However, the condensed disclosure period also puts significant pressure on a company to understand the degree to which it has been compromised and have a plan for mitigating the risk quickly. This may lead more companies to pay the ransom and confidently communicate a message to shareholders that they have done everything possible to mitigate the impact of the attack.

Finally, the SEC regulations put the role of chief information security officer (CISO) into the spotlight. The SEC enforcement action against the SolarWinds CISO demonstrates the personal downside that CISOs now face. CISOs should protect themselves accordingly.

CISO Liability in Focus: SEC Enforcement, Insurance, and [Personal] Risk Mitigation

The SEC is ratcheting up the pressure on CISOs—and it's entirely deliberate. Get insights into what companies can do to protect their CISOs.

2.3 AI's Impact on Cyber Risk

Artificial Intelligence (AI) is transforming business at breakneck speed across nearly every industry. As with most new technologies, the use of and reliance on a piece of technology carries with it increased cyber risk. AI is no different.

Many companies will incorporate AI technologies into their internal processes or external products in 2024. As a tool, AI can power companies to produce more of their products or services faster, creating more revenue, but also more opportunities for error.

Similarly, AI-powered cybersecurity tools will be used to protect organizations. Hackers will leverage AI to further their own causes. The battle will continue as it does today—with each side having an upper hand at different times.

Inherently, AI won't change cyber risk. But it may exacerbate the severity of a problem when it arises. This will increase the importance of making an informed choice using data science and analytics when purchasing cyber insurance.

Artificial Intelligence: Practical Considerations for Boards and Management Teams

Artificial intelligence poses great opportunities for companies—as well as significant risks and challenges. Discover what company leaders need to know as their employees begin to use AI.

2.4 Continued Focus on the Technology Supply Chain

Over the past few years, we have seen hackers focus on technology supply chain attacks—exploiting security flaws in widely adopted technology. Recent examples include breaches at SolarWinds; Kaseya; and Ipswitch, Inc.'s MOVEit file transfer protocol. These singular attacks led to a significantly larger number of data breaches resulting from the vulnerability being exploited at companies that used the hacked technologies.

The payoff for attackers is clear: breaching a single, widely used technology vendor can provide access to high volumes of potential targets. Add in the fact that many companies don't patch systems in a timely manner, and the effects of these breaches can be felt for years.

2.5 Pixel Tracking, CPRA, and Privacy Risks

Cyber regulation is not only the domain of the SEC—states have been trying to regulate consumer privacy rights since 2018. California led the charge, and it'll be in the spotlight again in 2024 when the California Privacy Rights Act of 2020 (CPRA) finally gets enforced. The delay in enforcement that occurred in 2023 isn't going to stop the inevitable. Violations of the law will result in increased enforcement actions and penalties for violating companies.

California isn't alone in this trend—there are now 13 states with state privacy laws on the books, including Texas.

Companies also find themselves playing catch-up to regulators in disclosing what data they collect, how they collect it, and what it is used for within their business. Pixel tracking claims are the latest target for the plaintiffs' bar—going after companies tracking website activity through pixels on the screen without obtaining proper consent. While the focus was on healthcare companies in 2023, expect more lawsuits to be filed in other industries, such as retail and financial services, in 2024.

Examining the Difference Between CPRA and CCPA Regulations

Get the details on how the CPRA built upon the existing California Consumer Privacy Act of 2018 (CCPA) framework and improved on the original legislation.

3.0

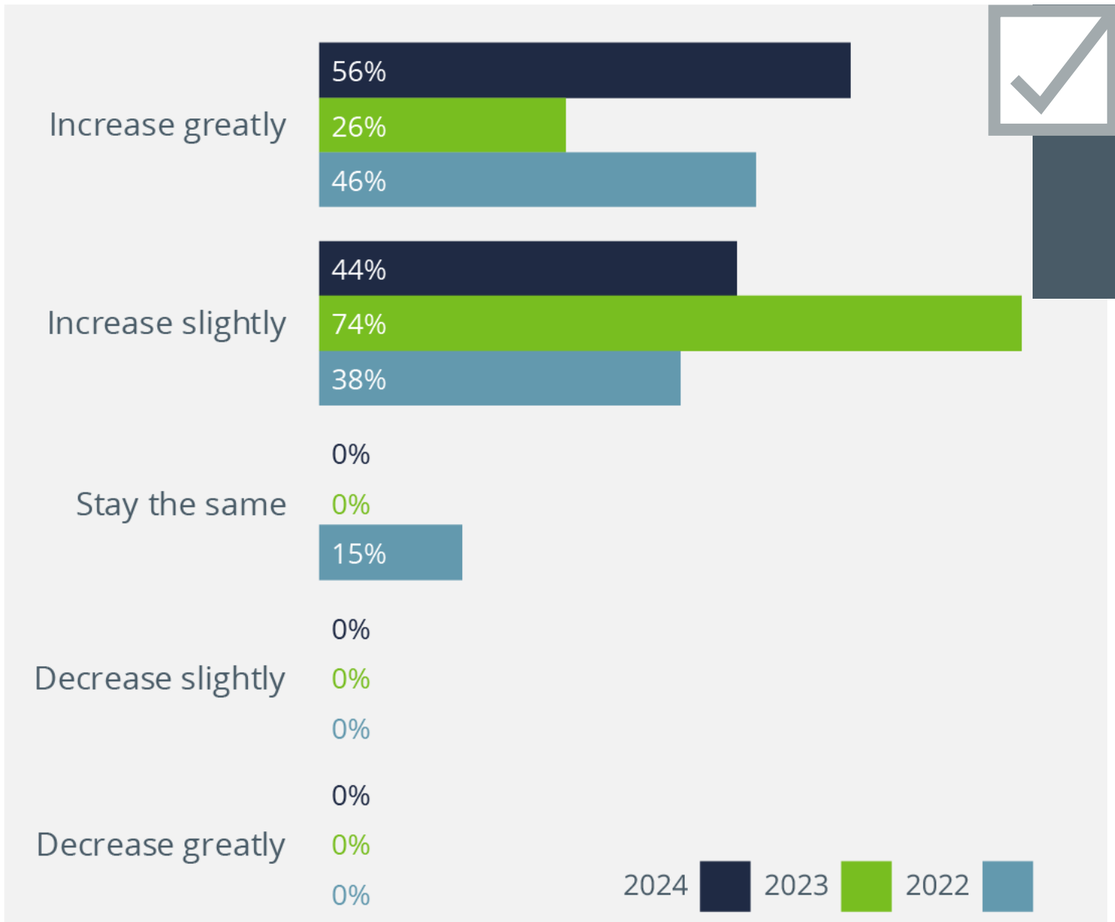
Underwriters' Survey

Good brokers are not just mere intermediaries; they are fierce advocates for their clients. Not only that, but they're also attuned to the pulse of the insurance carrier world. At Woodruff Sawyer, we engage in daily conversations with insurance carriers to gain a deeper understanding of their perspectives.

In our annual survey of cyber insurance carriers, we sought underwriter perspectives on the current risk environment,their risk appetite, and future pricing expectations. We surveyed a diverse range of insurance carriers, from established domestic carriers to Lloyd's syndicates and startup MGAs. The results offer a glimpse into the minds of underwriters and the cyber insurance landscape for 2024.

Start >>

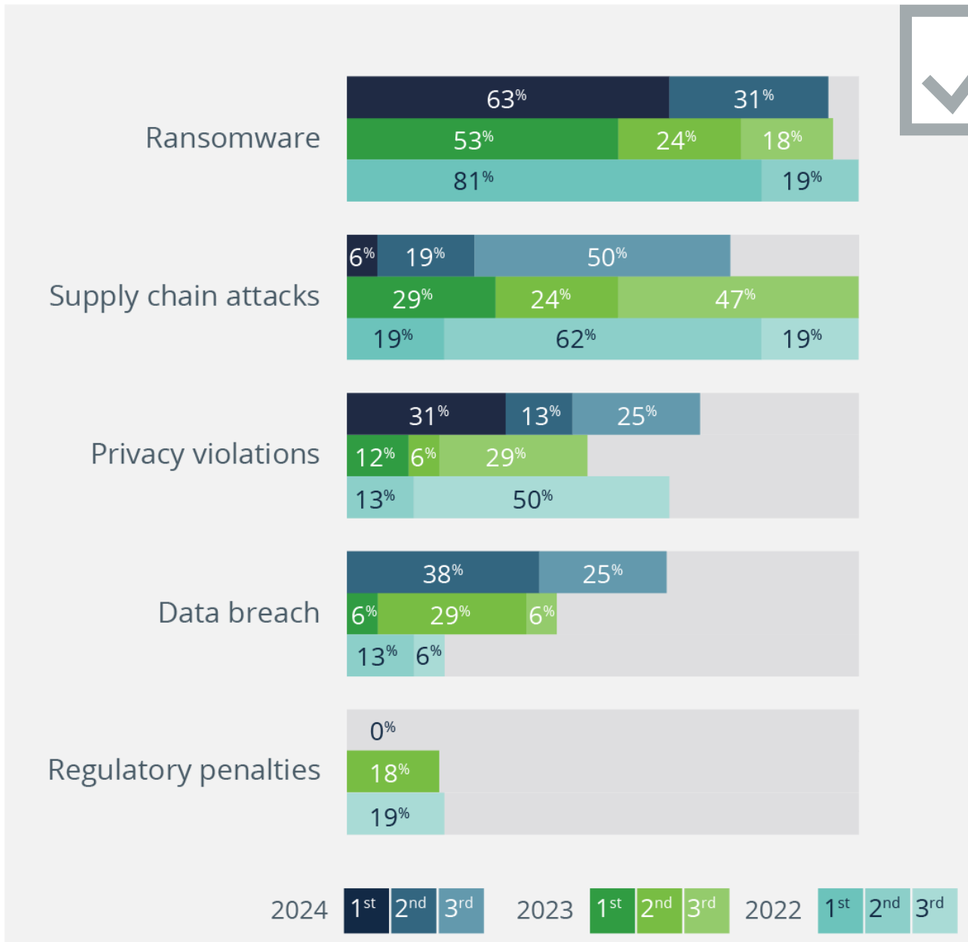
Q1 Over the next 12 months, will cyber risk:



56% of underwriters believe cyber risk will **increase greatly** in 2024

All underwriters surveyed think cyber risk will increase in 2024. The percentage of respondents who believe cyber risk will "increase greatly" in 2024 doubled compared to last year, reflecting heightened concerns within the industry.

Q2 What is the most concerning threat companies face? (Ranked)



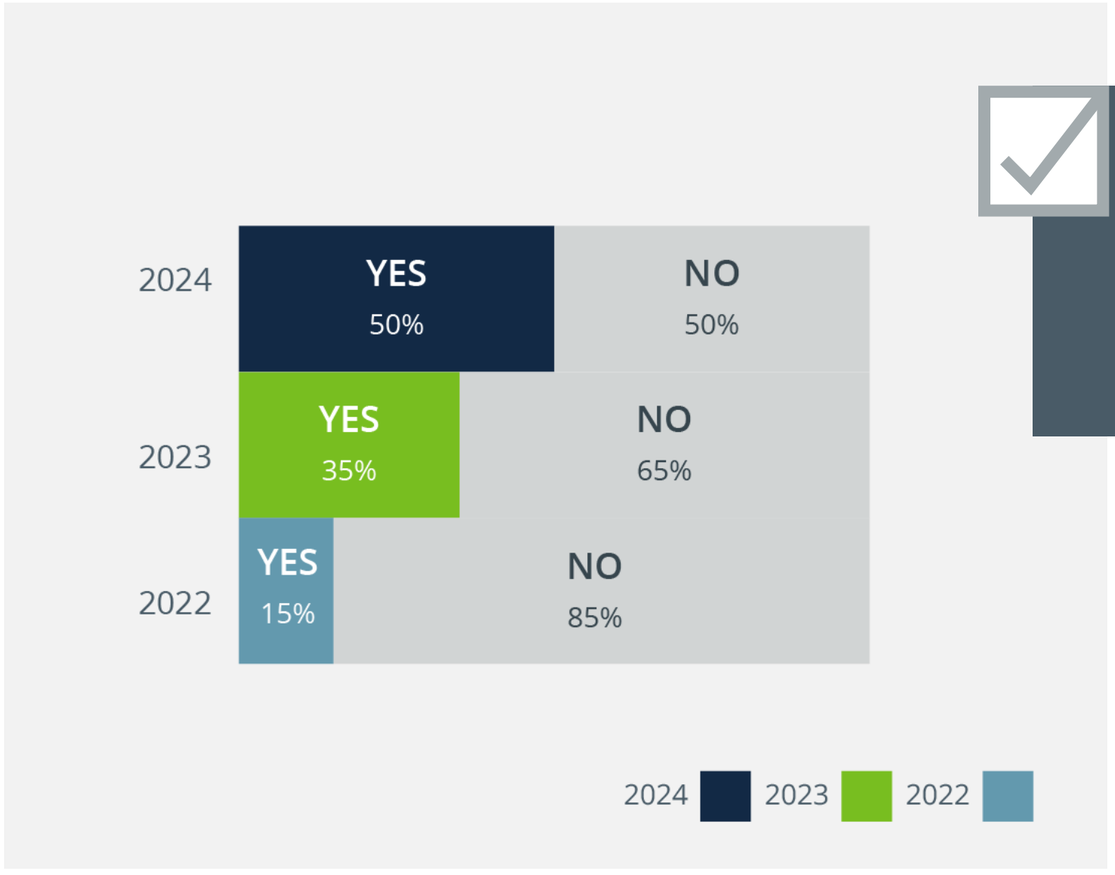
63% of underwriters ranked **ransomware** as the **number one threat.**

Ransomware maintains its status as the most significant threat for underwriters. This year marks a notable shift in concerns, with privacy violations and data breaches gaining prominence compared to last year.

Other concerns noted by underwriters include:

- Generative artificial intelligence
- Business email compromise leading to significant losses

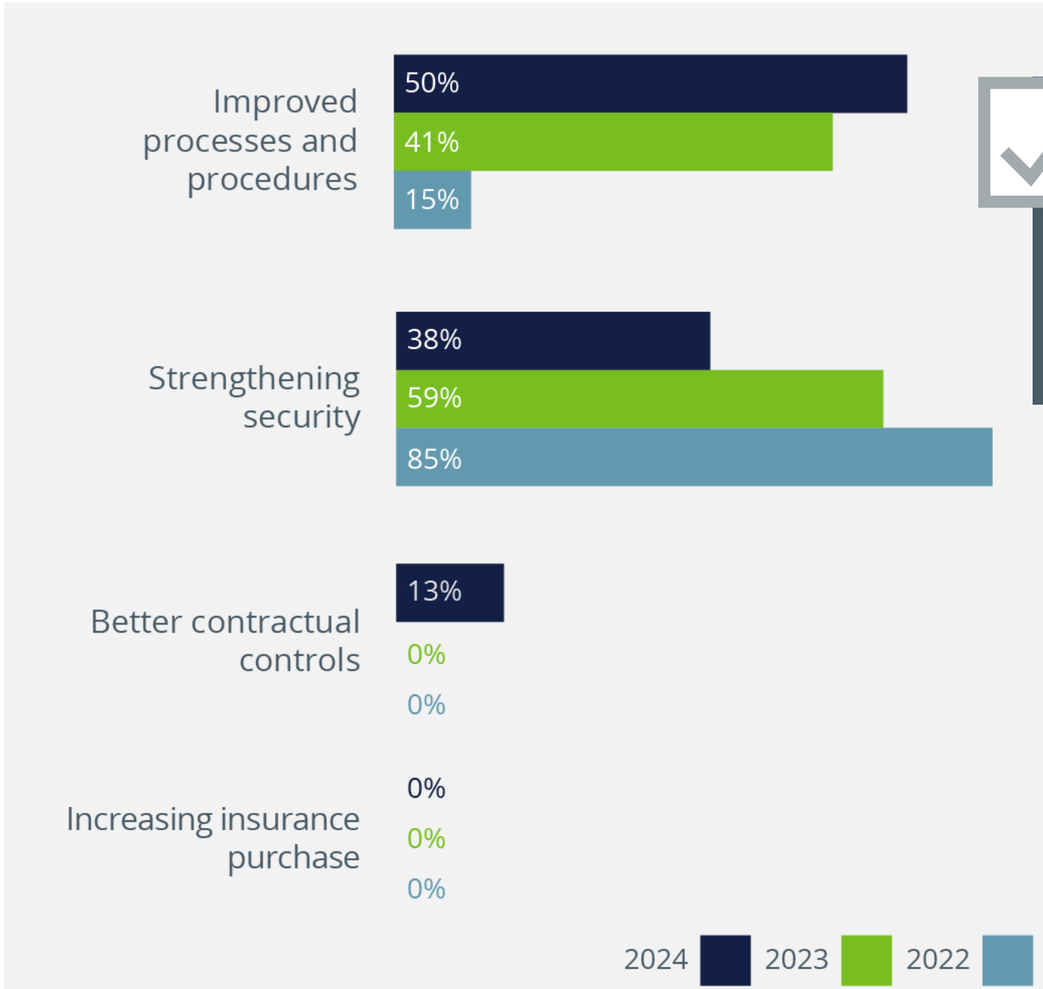
Q3 Are companies as aware as they should be about the cyber risks they face?



50% of insurers believe companies should be **more aware** of their cyber risk.

The survey suggests uncertainty or differing perspectives among underwriters, with an even 50%–50% split on cyber risk awareness. An increasing percentage of underwriters believe companies are becoming more aware of the cyber risks they face compared to prior years, but there is still a need for improvement in overall awareness.

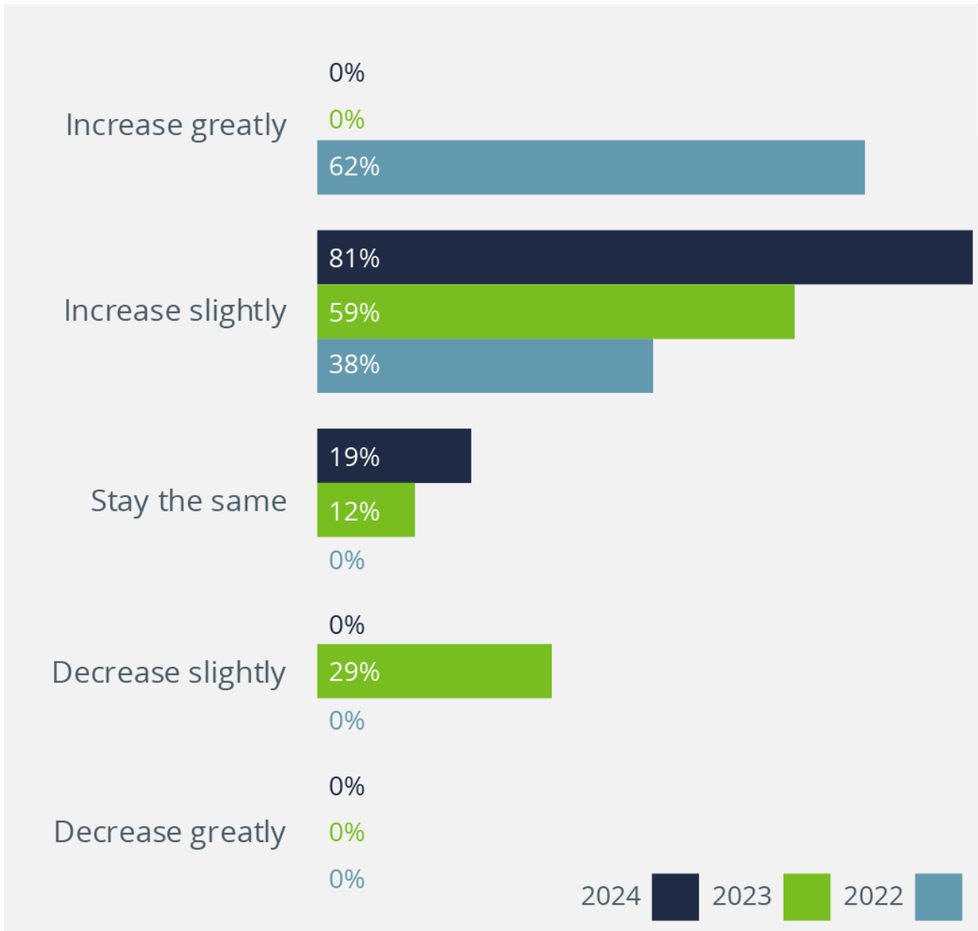
Q4 Which risk mitigation strategy needs the most focus from companies over the next 12 months?



50% of underwriters believe companies should focus on **processes and procedures**

The survey reveals a shift in risk mitigation priorities, with a decrease in emphasis on strengthening security (from 59% to 38%) compared with last year's survey. Improvement of processes and procedures remains crucial at 50%, while better contractual controls are becoming relevant.

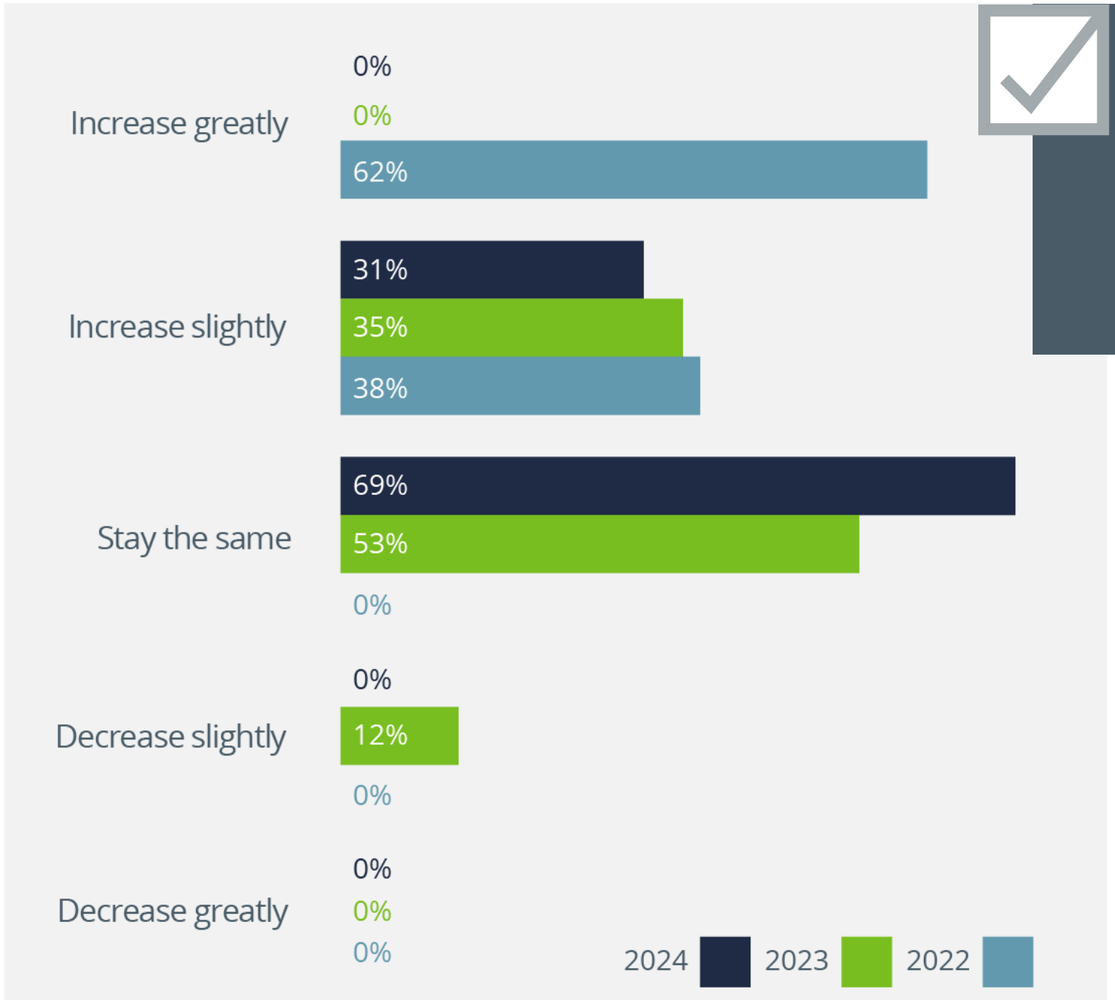
Q5 Industry-wide, over the next 12 months, how do you expect cyber insurance premiums to change?



81% of underwriters believe cyber insurance **premiums** will **increase** slightly.

A rising percentage of underwriters believe cyber insurance premiums will increase slightly, up 22 percentage points from last year. Only 19% expect premiums to remain unchanged, while none foresee a decrease. This suggests a notable industry shift toward higher premiums amid growing cybersecurity concerns.

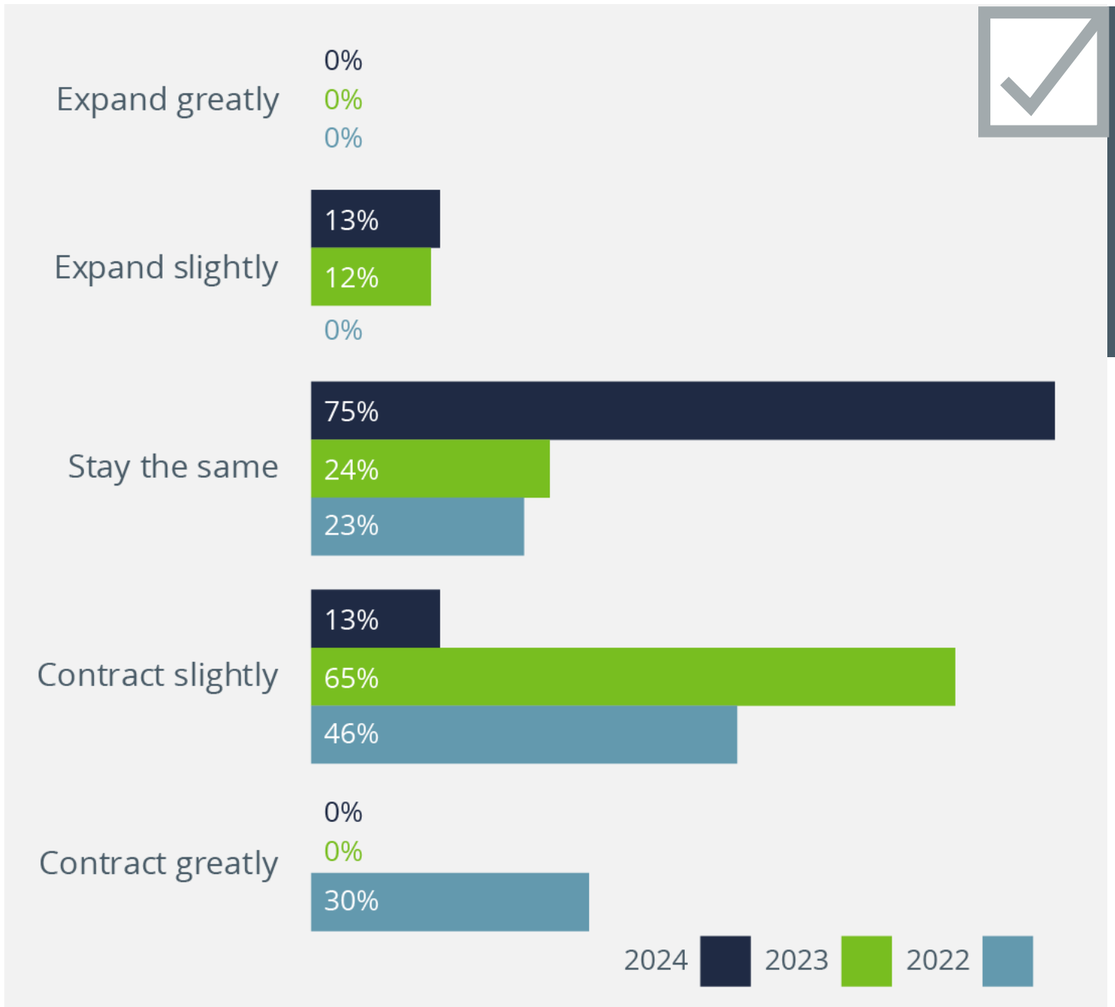
Q6 Industry-wide, over the next 12 months, how do you expect cyber self-insured retentions to change?



69% of underwriters expect **self-insured retentions to stay the same.**

This year's survey reveals a notable trend in cyber self-insured retentions (SIRs), with 69% of underwriters expecting them to remain unchanged, compared to 53% the previous year. Additionally, 31% anticipate a slight increase in SIRs, signaling a shift in industry expectations toward greater stability or a modest rise in the coming 12 months, with no underwriters foreseeing a decrease.

Q7 Industry-wide, over the next 12 months, how do you expect cyber coverage to change?



75% of respondents believe cyber policy **coverage** will **stay the same.**

This year's survey indicates a substantial shift in expectations for cyber policy coverage, with 75% of underwriters anticipating it to remain unchanged, compared to 24% the previous year. A smaller percentage (13%) expect it to contract slightly, while another 13% foresee a slight expansion, reflecting a notable industry-wide adjustment towards stability and moderation.

Q8 In the next 12 months, how do you expect cyber coverage to expand?

Respondents noted the following areas of expansion:

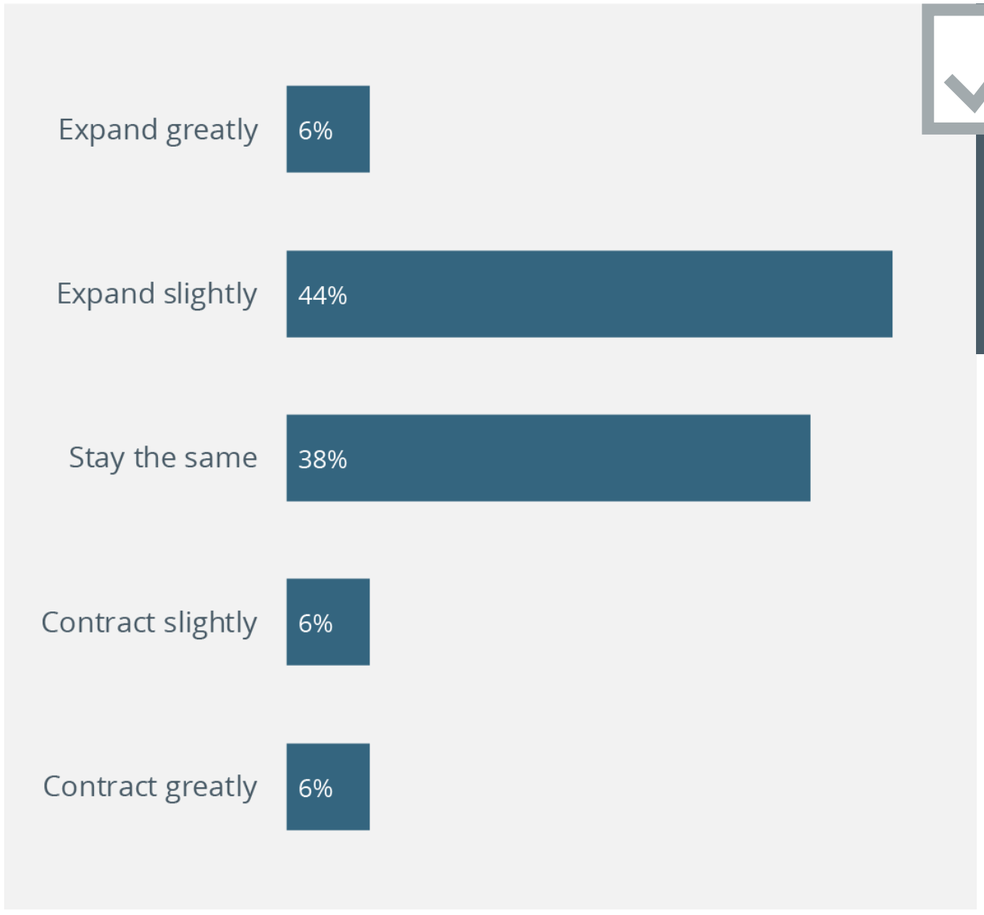
- Replacing insurance product deficiencies that need improvement
- Into the blended space misc/tech
- Targeting public officials, municipalities, and universities
- Additional security services
- Eased restrictions from the hard market, fewer sublimits
- Focus on privacy, with lower sublimits

Q9 In the next 12 months, how do you expect cyber coverage to contract?

Respondents noted the following areas of contraction:

- War exclusion
- Sublimits reappear
- Privacy claims exposure

Q10 Industry-wide, over the next 12 months, how do you expect underwriting scrutiny to change?



44% of respondents expect underwriting scrunity to **increase slighty.**

This year's survey indicates a prevailing expectation (44%) for underwriting scrutiny to increase slightly over the next 12 months. This may be bad news for insurance buyers already frustrated at the amount of information required to complete a cyber insurance application. However, it does prove the trend of higher scrutiny has staying power. With a risk as complex as cyber, higher underwriting scrutiny will become the norm.

2024 Cyber Insurance Landscape

According to Underwriters

56%
of underwriters believe
cyber risk will **increase greatly** in 2024.

81%
of underwriters believe
cyber insurance premiums
will **increase slightly** in 2024.

75%
of respondents believe
cyber policy coverage
will **stay the same**.

69%
of underwriters expect
self-insured retentions
to stay the same.

50%
of underwriters believe
companies should focus on
processes and procedures.

50%
of insurers believe
companies should
be more aware of
their cyber risk.

63%
of underwriters ranked
ransomware as
the number one threat.

44%
of respondents expect underwriting
scrunity to **increase slightly**.

4.0

Expert Insights

Lauri Floresca
Senior Vice President, Cyber Liability

Stephen Quintana
Senior Vice President, Cyber/E&O/Media Liability

Priya Cherian Huskins
Senior Vice President, Management Liability

David Anderson
Vice President, Cyber Liability

Start >>

4.1 For Public Companies, Incident Response Just Got Even More Difficult

Lauri Floresca

Senior Vice President,
Cyber Liability
Reach out to Lauri

How have companies been responding to the SEC's cyber disclosure rules?

The Securities & Exchange Commission (SEC) finalized its long-delayed cyber disclosure rules in late summer 2023, and the rules were tested almost immediately when three major public companies battled against significant ransomware threats in August and September. The new rules require companies to issue an 8-K form within four days of determining that a cybersecurity event is material, adding a new and difficult task during the already-complex process of responding to a cybersecurity incident.

Clorox, MGM Resorts, and Caesars Entertainment each released public statements with varying degrees of specificity during their attacks, and MGM and Clorox have since filed a second 8-K with more detail.

Many groups, including the SEC, shareholder plaintiffs' attorneys, and even the bad actors themselves will heavily scrutinize these statements once the companies issue them. The bad actors may even choose to publicly contradict the company's account or change tactics based on what they learn from the disclosures.

The challenge of determining materiality and crafting a thoughtful disclosure in such a short time is significant, and companies should build this task into their incident response planning and tabletop exercises. Companies will also need to have a good understanding of how their cyber insurance program may respond to incidents so they can include commentary on potential insurance recoveries.

4.2 Cyber Analytics Becomes a Much-Needed Tool

Stephen Quintana
Senior Vice President,
Cyber/E&O/Media Liability
Reach out to Stephen

How can analytics help companies make better decisions about their cyber risk and insurance?

In this data-driven world, companies are leaning on analytics to make informed decisions in many areas of capital allocation and risk management. It's no different for those companies concerned about the ever-present risk of cyberattacks—they're trying to understand the level of risk they face and how these risks should inform insurance purchasing decisions.

As ransomware attacks persist and privacy requirements increase due to domestic and international regulations, companies are forced to continue reevaluating their exposure to cyber and privacy risks. Useful cyber loss modeling and analytics can provide context to help drive decisions on investment and risk appetite.

Specifically, cyber analytics can be used to:

- Quantify and assess the impact of different cyberattack scenarios on a business
- Provide guidance on what amount of cyber insurance to purchase
- Provide context to determine what level of self-insured retention aligns with a company's risk tolerance
- Evaluate whether and where the insurance marketplace is charging more or less than the expected cost of risk for a given business

Cyber analytics is an essential tool for businesses when making decisions about cybersecurity insurance. By using the right analyses, businesses can better assess and quantify cyber risks to select reasonable cyber insurance limits and retentions that align with their risk tolerance strategy.

4.3 The Pressure on CISOs Increases

Priya Cherian Huskins, Esq.
Senior Vice President,
Mangement Liability
Reach out to Priya

How can CISOs protect themselves from the bankrupting cost of litigation?

Most chief information security officers (CISOs) took their jobs without ever imagining they might be in the line of fire for securities class action litigation or even enforcement actions by the SEC and criminal prosecutions by the DOJ—and here we are. Indeed, with the SEC's newly released rules on cyber disclosure, the pressure on CISOs continues to increase.

First, the good news: Directors and officers (D&O) insurance policies for public companies can cover CISOs for things like being named in securities litigation or the object of an enforcement action or criminal prosecution. In some cases, coverage will be automatic. In others, there is work to be done. In all cases, CISOs will want to make sure they are covered by a company's D&O insurance policy as broadly as possible.

Second, CISOs should ask for personal indemnification agreements. This is an agreement between a company and an individual in which the company promises to do things like advance legal fees and, where allowable, pay settlements if an individual is being sued. CEOs, CFOs, and general counsels routinely get these. All things considered, it makes sense for CISOs to start asking for personal indemnification agreements as well.

CISO Liability in Focus: SEC Enforcement, Insurance, and [Personal] Risk Mitigation

Read about the recent SEC charges filed against the SolarWinds CISO and how companies can protect their own CISOs.

4.4 Coverage for Cyber Physical Damage Continues to Evolve

David Anderson
Vice President,
Cyber Liability
Reach out to David

Will cyber physical damage coverage continue to become more limited?

Over the last five years, major global insurers underwent extensive internal audits on their non-cyber portfolios—such as property, marine, stock throughput, product liability, and casualty policies—to identify and exclude any unintentional or unexpected "silent cyber" losses arising from a cyber event. The result: Nearly all insurers have imposed broad cyber exclusions on property, casualty, marine, and other policies vis-à-vis Lloyd's LMA wordings, excluding coverage for loss or claims arising out of a cyberattack causing physical damage or bodily injury. Some insurers are also inserting additional clarification to exclude coverage for damage to operational technology, industrial control systems, and other electronic data processing equipment that would otherwise be covered for non-cyber-related fire, explosion, or other resultant damage to tangible property.

Additionally, the confluence of "state-sponsored attack," "widespread event," and "non-utility infrastructure" exclusions continue to narrow the scope of coverage for bodily injury and property damage within an insured's entire insurance portfolio.

We expect market-leading global reinsurers to further restrict whatever limited coverage is still embedded for these perils in 2024, which directly impacts direct insurers' ability and appetite to cover these risks within traditional insurance policies.

4.4 Coverage for Cyber Physical Damage Continues to Evolve (cont.)

Will cyber physical damage coverage continue to become more limited?

To address this issue, an international market with over 15 insurers (and growing) has emerged, with both cyber and property and casualty (P&C) underwriters who can affirmatively cover these excluded perils with policies that dovetail with your company's P&C and cyber insurance programs to provide clear, delineated, and targeted coverage.

Exploring Cyber Insurance and Its Intersection with Property Coverage

Delve into the numerous risk transfer solutions that can be used to address this coverage gap.

5.0

Concluding Perspective

Start >>

Carolyn Polikoff

President of Commercial Lines

415.402.6513 | cpolikoff@woodruffsawyer.com

View Bio

LinkedIn

At the beginning of last year, we celebrated a normalizing insurance market, and the data supports our projections. In 2023, most of our cyber clients experienced decreased pricing when renewing their policies. Stronger cybersecurity controls have helped contribute to this trend, as more carriers are willing to offer insurance.

However, the cyber insurance market continues to evolve—the industry constantly faces new and serious risks. External factors continue to affect the market, including wars, federal and state regulations, and the rise of artificial intelligence. The insurance market has responded with an unclear war exclusion and coverage restrictions for systemic risk and privacy violations, while companies struggle with timely disclosures to avoid enforcement actions and lawsuits.

In addition, companies are dealing with alarming levels of ransomware—claims rose in 2023, reaching the record-setting levels set in 2021.

Underwriters in our annual survey think cyber risk will increase greatly in 2024—more than half think this is the case, a higher percentage than last year. Most also think premiums will increase slightly, while unfortunately, no one expects decreased premiums.

As the market shifts, companies must understand their changing risks and adjust accordingly. One way to stay on top of changes: this annual *Cyber Looking Ahead Guide*, where we aim to give you clarity on the trends that affect your insurance coverage and rates.

At Woodruff Sawyer, we understand the cyber liability challenges businesses face today. Our team of experts is dedicated to safeguarding our clients against these risks by providing them with valuable insights and education. With our extensive expertise and experience in this specialty line, we leverage data to empower our clients to make informed decisions about their cyber risk management strategy and insurance programs. If you have any questions or concerns about mitigating and transferring cyber risk, or any of the data in this *Guide*, our experts are here to provide you with the answers and guidance you need.

About Woodruff Sawyer

As one of the largest independent insurance brokerage and consulting firms in the US, Woodruff Sawyer protects the people and assets of more than 4,000 companies. We provide expert counsel and fierce advocacy to protect clients against their most critical risks in property and casualty, management liability, cyber liability, employee benefits, and personal wealth management. An active partner of Assurex Global and International Benefits Network, we provide expertise and customized solutions to insure innovation where clients need it, with headquarters in San Francisco, offices throughout the US, and global reach on six continents.

Subscribe for Expert Advice and Insights

Sign up to receive expert advice, industry updates, and event invitations related to Cyber Liability.

Additional Resources

- Cyber Notebook
- D&O Notebook
- Woodruff Sawyer Insights
- Woodruff Sawyer Events

For more information

Call 844.972.6326, or visit woodruffsawyer.com

Find out why clients choose to work with Woodruff Sawyer.