WOODRUFF SAWYER

Looking Ahead

Cyber Insurance Trends for 2023

Start >>

Table of Contents

1.0

Cyber Market Update

Start >>

Dan Burke
Senior Vice President,
National Cyber
Practice Leader
Reach out to Dan >>

1.1 US Market Update

After two years of price increases, the cyber insurance market is normalizing as we head into 2023. Insurance carrier loss ratios are healthier now than they have been in the past few years—a result of price increases and a downturn in the frequency of ransomware attacks throughout 2022. Some in the industry attribute the lower ransomware activity to Russian attackers' focus on the war efforts in Ukraine—and predict that ransomware will rise again when the war effort subsides.

Let's dive into some other trends in the cyber insurance market.

Technology E&O Capacity Remains Constrained

While stand-alone cyber policies have benefitted from an easing of the capacity crunch in 2022, the insurance market for technology errors and omissions (E&O) remains tighter than normal. Legal concerns and regulatory activity around consumer privacy rights are keeping many insurance carriers on the sidelines, limiting capacity and driving tougher insurance renewals.

Coverage Restrictions for Systemic Risk

There is no hotter topic in the cyber insurance space than systemic risk—or the risk of a single vulnerability impacting thousands of companies all at the same time. This risk is being addressed by nearly every cyber insurance carrier at the urging of their re-insurance partners. Systemic risk shows itself in two primary ways: aggregation risk and widespread events. This is one area where we expect to see coverage restricted throughout 2023.

Continued Focus on Security Controls

Underwriters continue to over-index their view of risk towards the cybersecurity controls in place at a company. The exact controls underwriters look for is a moving target, often confounding companies that have made significant investments in cybersecurity over the past year. Expectations heading into 2023 include next-generation improvements on some familiar security concepts.

Cyber Insurance Requirements: The Next Frontier >>

Cybercriminals are bypassing existing layers of security using advanced tactics and continuously adapting their techniques. Learn the seven controls that can help bolster your company's cybersecurity.

1.2 Pricing Trends

While prices remained elevated and increased over 2021 pricing throughout the year, we have seen the level of increase tail off in Q4 of 2022, which bodes well for the prospect of a normalized market in 2023. We don't expect price decreases for most buyers, but rather more moderate price increases.

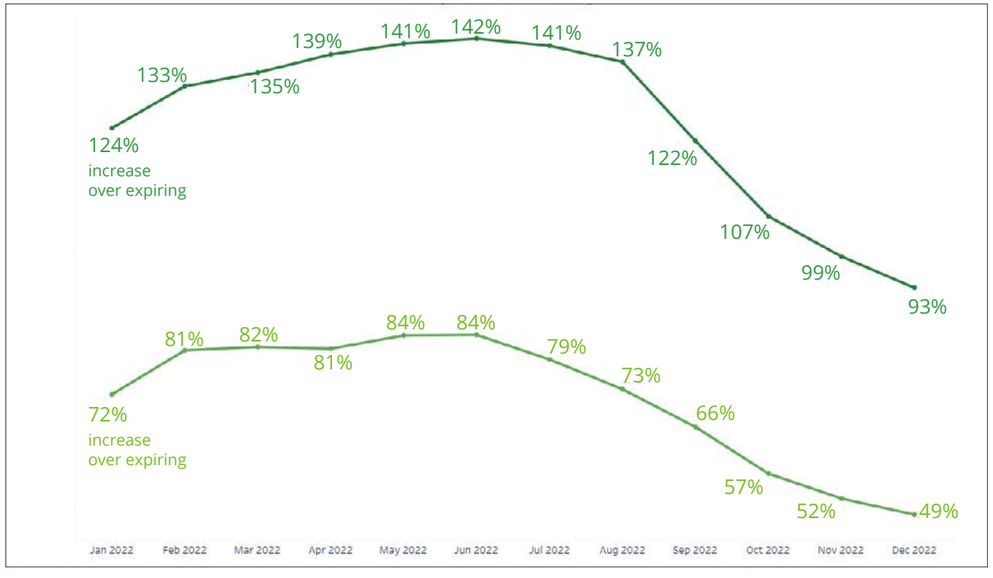
Excess insurance pricing has stayed consistent throughout the year. Last year, the excess hard market started first, with excess rates jumping and the primary market following. In 2022, excess pricing remained consistent throughout the year. However, this relatively flat excess pricing environment is still good news for insurance buyers. If the excess pricing environment continues to be a leading indicator of the primary pricing environment, 2023 pricing should continue to soften throughout the year.

Cyber insurance pricing continued to heat up throughout 2022, although signs of a normalizing market appeared in the 4th quarter.

Cyber Liability Insurance Buying Guide >>

Learn how to better identify your cyber risks, understand what cyber insurance covers, and see how a comprehensive approach best protects your organization.

Cyber Price Trends for 2023



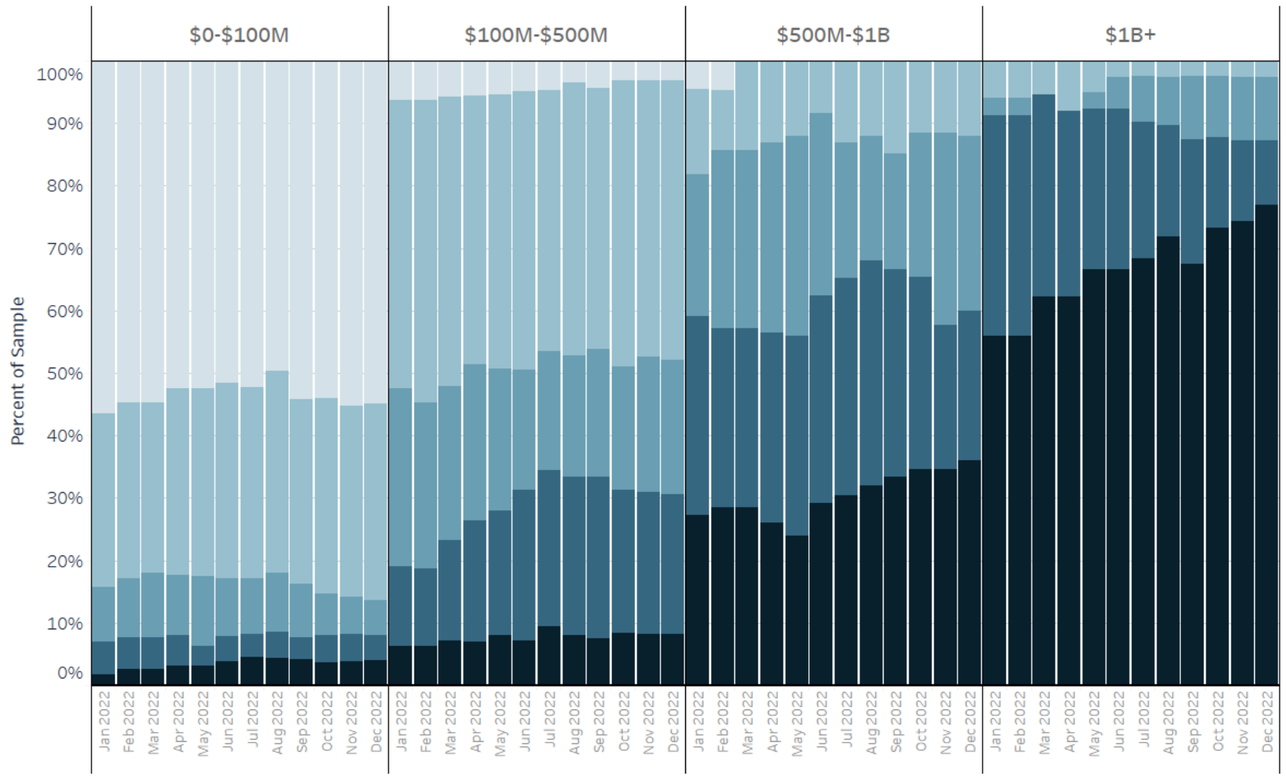
Median Third Quartile – the highest paying quartile in our sample

1.3 Self-Insured Retention Trends

Insurance carriers view cyber risk as increasing. As a result, they've not only increased premiums but also asked companies to keep more risk on their balance sheets in the form of self-insured retention (SIR) increases. Woodruff Sawyer clients with more than $100 million in revenue have seen retention increases over the past 12 months.

Companies with over $100 million in revenue have seen increases in self-insured retentions over the last 12 months.

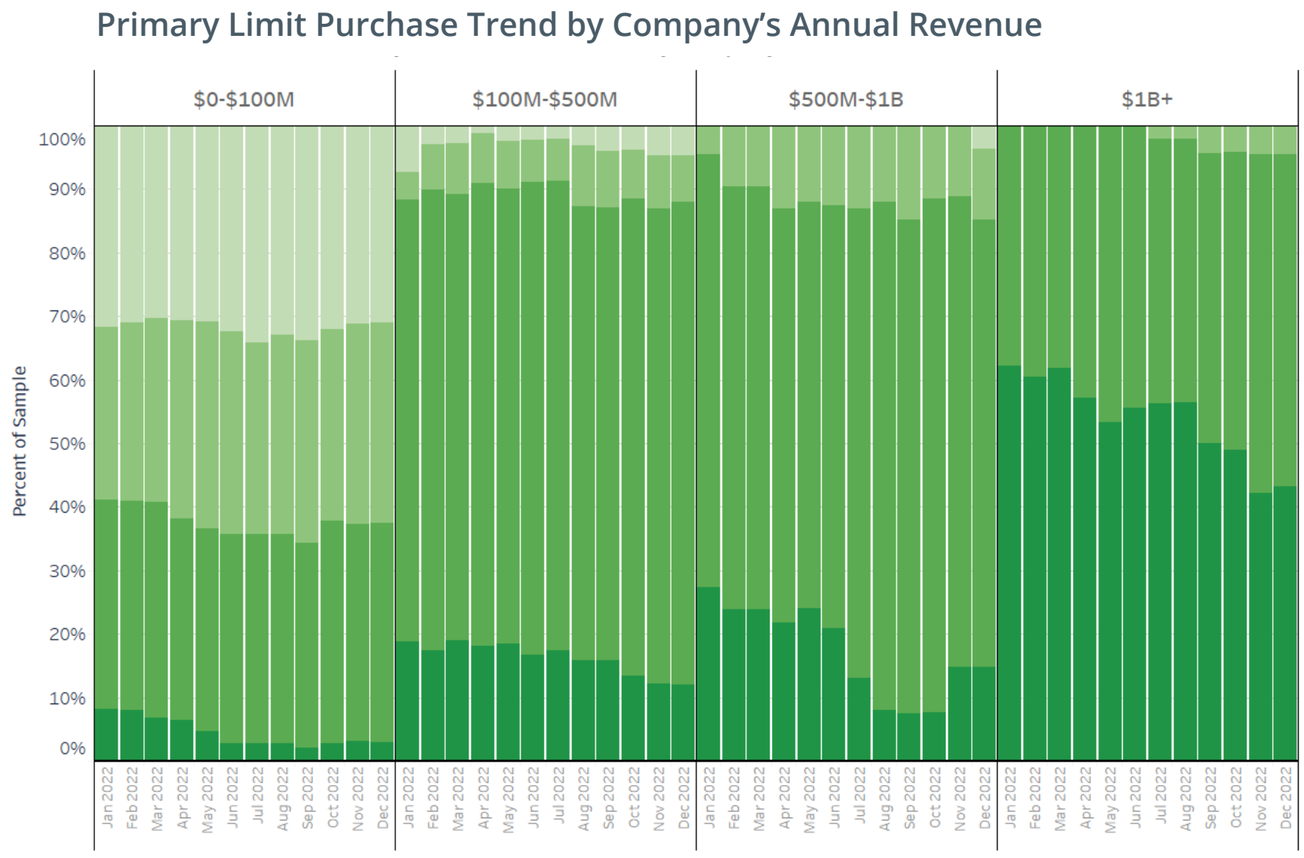
Self-Insured Retention Trend by Company's Annual Revenue



1.4 Limit Trends

A trend we noticed throughout the hard market of 2021 was a lowering of limits by most insurance carriers from $10 million to $5 million for any one client. Thankfully, this trend of primary limit decreases subsided throughout 2022, and we began seeing a more stable limit profile for all revenue bands.

In the cyber insurance market, we've seen many carriers continue to offer a maximum of $5 million in limit for any one client.



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 Aggregation Risk

Aggregation risk is most prevalent for service providers—particularly those in the technology sector. This is the risk of a vulnerability in a company's technology product or service leading to a security incident for all its customers at the same time.

> A recent example of aggregation risk is the SolarWinds breach in 2020. Hackers infiltrated Solarwinds' software development life cycle, leading to a legitimate software update that included a backdoor vulnerability going out to their customers.

If normal cyber risk is the risk of your company suffering a security incident, aggregation risk is the risk of all your customers suffering a cyber incident and looking to you for recovery.

The best risk management for aggregation risk is strong contractual protections that include limitations of your liability. This is easier said than done when negotiating contracts.

2.2 Widespread Events

Widespread events are the alternate side of systemic risk from aggregation risk. This is the risk that all companies using a similar piece of technology are affected by the same vulnerability at the same time.

> An example of a widespread event is if vulnerabilities are found in common software, such as Microsoft Exchange Server software, which powers many corporate email systems.

Widespread event risk may be the most frustrating element of cyber risk for insurance buyers. There is very little a company can do to prevent being impacted by the widespread vulnerability—but it is impacting their insurance, nonetheless. Insurance carriers typically add a catastrophic load charge to the premium to account for the risk of a widespread event. More recently, they have been looking to limit coverage available for these scenarios by reducing the limits available under the policy for specific widespread events.

How a Cyber Attack Triggers Multiple Parts of a Cyber Security Insurance Policy >>

The ripple effects of a cyberattack can reach sensitive customer data and business continuity. Learn the interconnectivity between the different coverage elements and how they apply to a modern cyberattack.

2.3 C-Suite Liability for Cyber Incidents

The C-suite is being held accountable for cybersecurity failures at their companies. This isn't a new trend necessarily—CEOs and CISOs have lost jobs for major cybersecurity failures at many organizations over the years. However, today they also face the prospect of personal liability for those same cybersecurity failures.

> This trend has led to CISOs facing criminal liability for covering up security incidents or being named individually in shareholder class action lawsuits, and CEOs being personally held responsible for security improvements by the Federal Trade Commission.

Particularly for CISOs, this new trend is concerning and an aspect of their job they likely didn't consider when taking the role. The good news for them is that insurance is a solution for personal liability.

Cyber insurance typically includes coverage for individual employees of the company when named in lawsuits. Cyber insurance can even provide some coverage for defense costs if a CISO faces accusations of criminal conduct—up until the final, non-appealable adjudication of the case. In the case of shareholder class action lawsuits, a good directors and officers (D&O) insurance policy will cover the CISO if they are considered an officer of the company in the corporate charter and bylaws.

2.3 C-Suite Liability for Cyber Incidents

CISOs Under the (Liability) Gun >>

Chief information security officers (CISOs) face an increased likelihood of legal scrutiny after a significant breach. Read about recent examples and learn how to ensure CISO coverage for cyber breaches.

SolarWinds' Cyberbreach: Another Caremark Claim Dismissed >>

Stockholders sued SolarWinds corporate directors, alleging they failed to adequately oversee cyber risk and citing a Caremark violation. Learn why the court dismissed the lawsuit.

2.4 The War Exclusion and Nation-State Sponsored Hacking

The Russian invasion of Ukraine in 2022 raised the prospect of invoking the war exclusion in response to cyberattacks that might spill outside of the intended target in Ukraine. While the war exclusion hasn't been invoked on a cyber insurance claim to our knowledge, many cyber insurance carriers are raising the issue with the intent of providing clarity around what types of attacks constitute an act of war.

Some insurance carriers have fallen on the side of war being classified as nation-state attacks on other nation-state or government targets. Thus, an attack on a private-sector business would not invoke the war exclusion.

Other markets, notably Lloyd's of London, have come out more aggressively with their interpretation of when the war exclusion applies. Lloyd's believes that any attacks backed by a nation-state should not be covered by insurance—and has developed proposed wording for its syndicates to adopt stating as much.

The key issue with invoking the war exclusion is the attribution of an attack to a specific threat actor or group of threat actors. Attribution is a very difficult technical endeavor and rarely leads to black-and-white conclusions about who is responsible for an attack.

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.

2.5 Privacy Issues: Here Comes the CPRA

In the 2020 election, California voters approved a measure to codify the law around consumer privacy rights, introducing the California Privacy Rights Act (CPRA) to replace the 2018 California Consumer Privacy Act (CCPA) law. While the CPRA maintains the private right of action against companies that suffer a data breach, it also increases the likelihood of penalties for law violations.

Notably, the CPRA takes enforcement off the desk of the California Attorney General and places it into the hands of a newly created agency, the California Privacy Protection Agency. The CPRA also removes the 30-day "cure" period, which allowed violating companies to fix the issues causing their violation before being subject to a penalty. These two changes portend more enforcement as the law becomes operational on January 1, 2023.

New California Privacy Laws: Get Ready (Again) >>

Learn more about California's new consumer privacy law and changes to the prior law that will affect businesses.

3.0

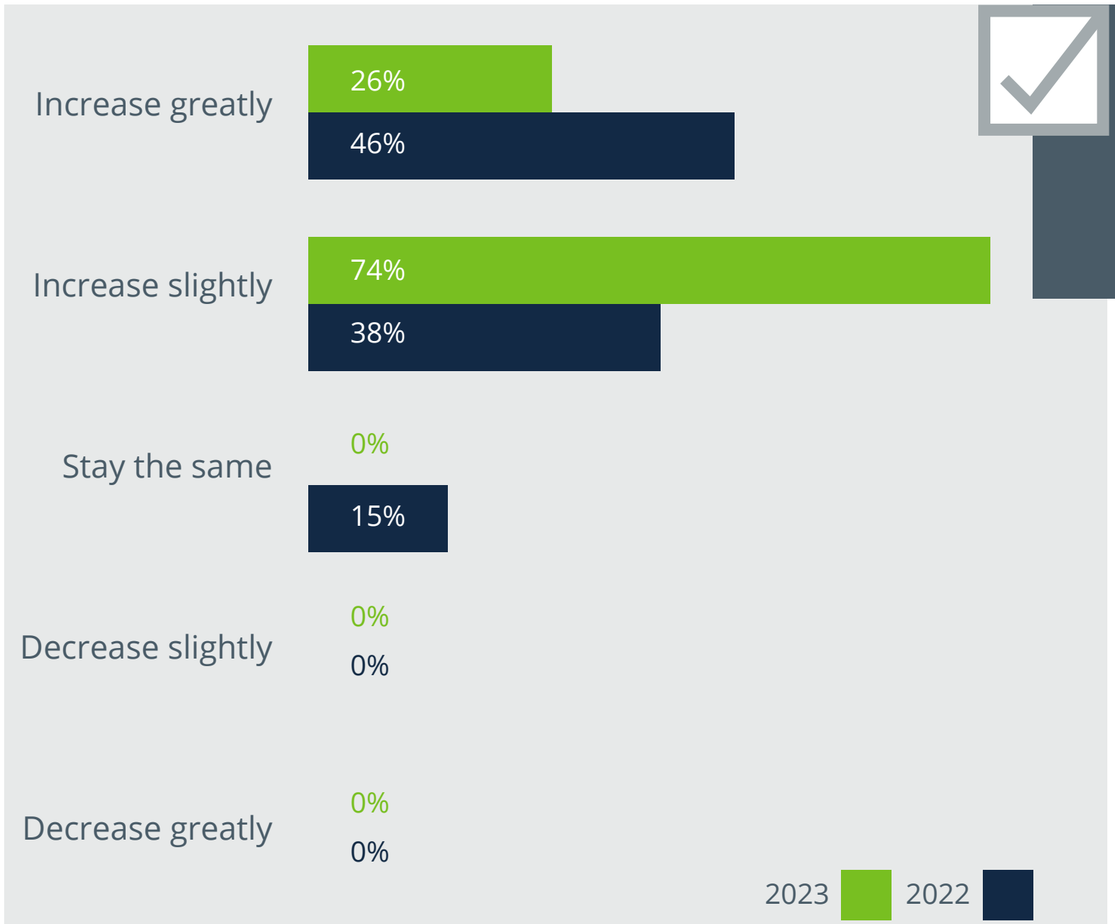
Underwriters' Survey

Good brokers are first and foremost advocates for their clients. As part of this advocacy, good brokers also listen to their insurance carrier partners to better understand their views of the world, including their current appetite for risk. Woodruff Sawyer is in conversation with insurance carriers every day. For this section of *Cyber Looking Ahead*, we surveyed insurance carriers with whom we place cyber insurance around the world—from domestic carriers to Lloyd's syndicates to startup MGAs.

We asked questions regarding the current risk environment, risk appetite, and future pricing expectations. The results illuminate the expectations of underwriters for 2023.

Start >>

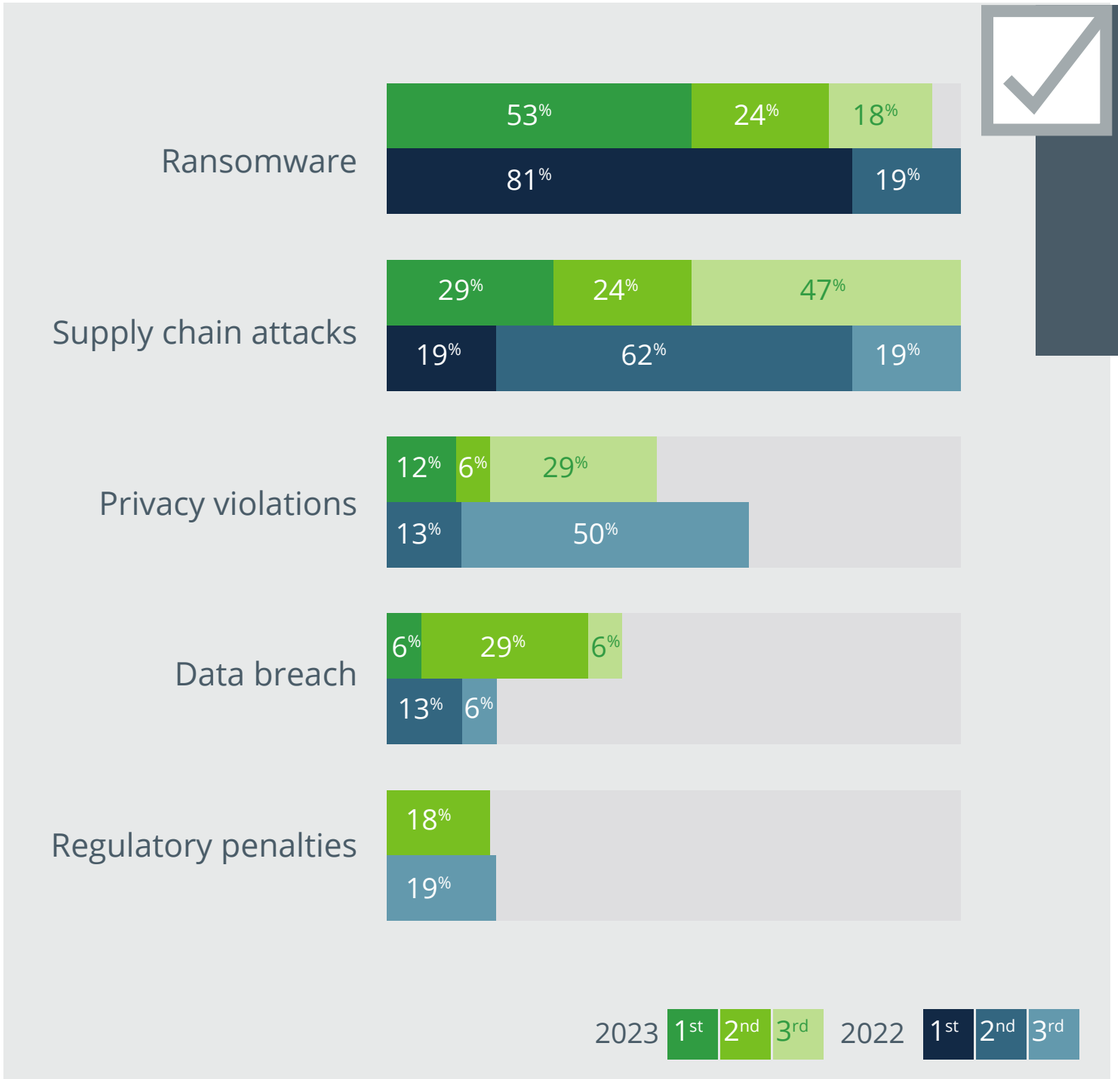
Q1 Over the next 12 months, will cyber risk:



26% of underwriters believe cyber risk will **increase greatly** in 2023

All underwriters surveyed think cyber risk will increase in 2023. However, a lower percentage of respondents believe it will "increase greatly" compared to last year.

Q2 What is the most concerning threat companies face?

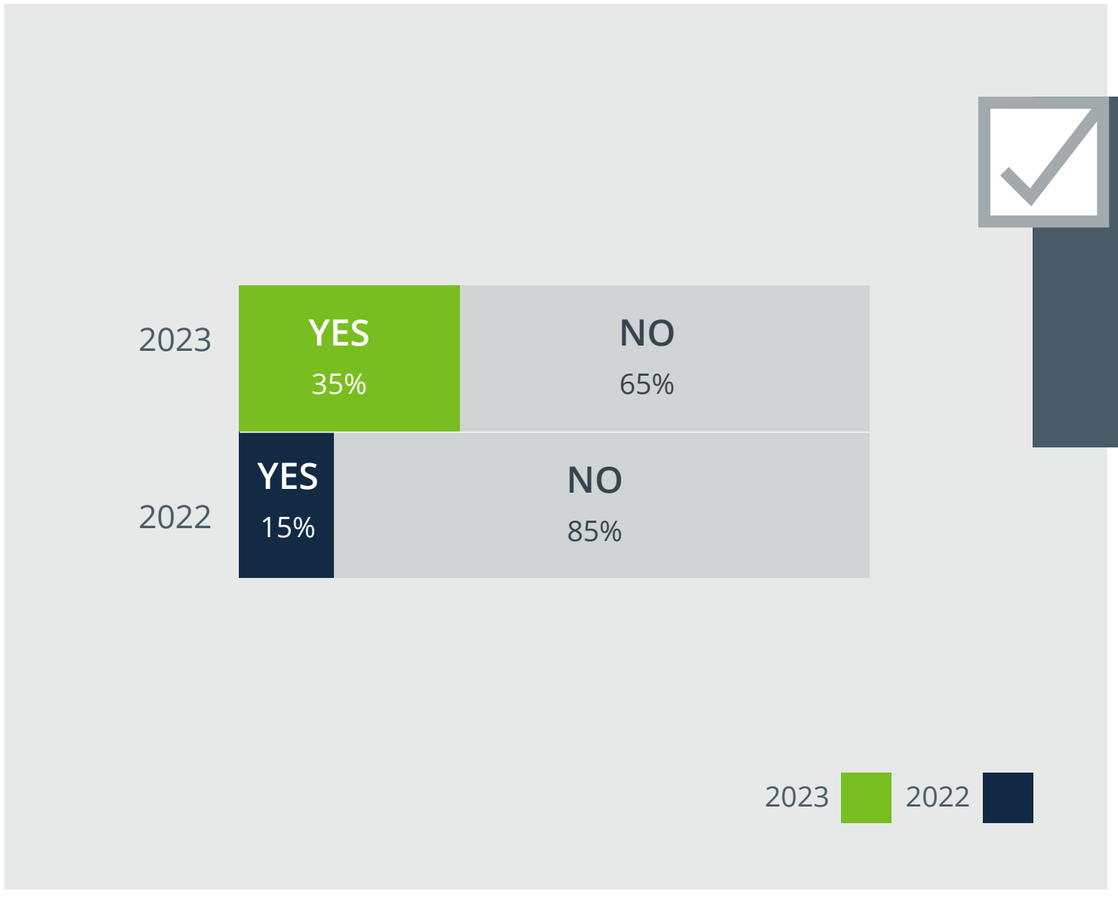


53% of underwriters ranked **Ransomware** as the **number one threat.**

Ransomware continues to rank as the highest cyber threat. Privacy violations have overtaken data breaches as more concerning overall to underwriters—and yet a higher share of underwriters ranked data breaches in their top two concerns. Other concerns noted by underwriters include:

- Behavioral marketing risks, such as wrongful collection and use of data for marketing purposes
- Systemic events
- Business email compromise attacks.

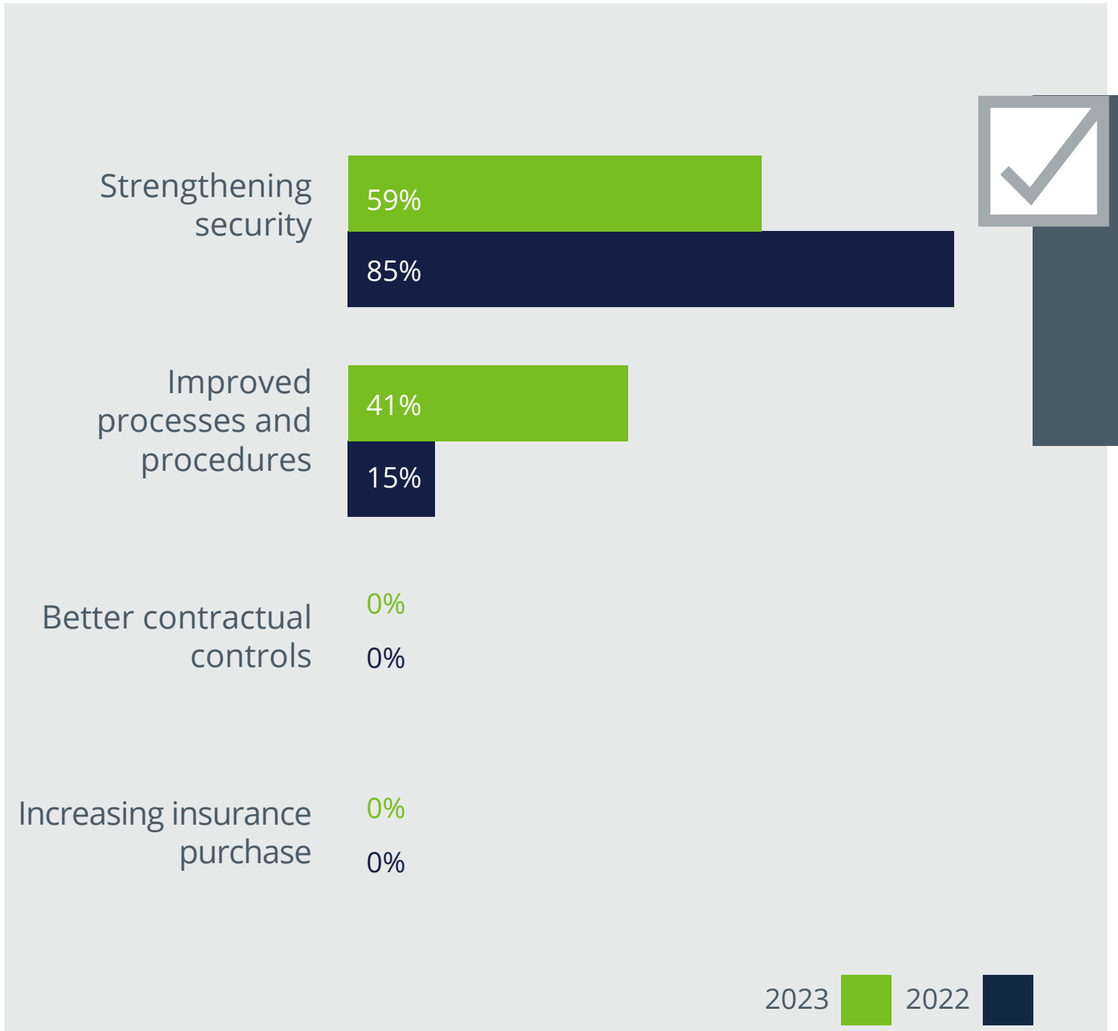
Q3 Are companies as aware as they should be about the cyber risks they face?



65% of insurers believe companies should be **more aware** of their cyber risk.

Underwriters think companies are becoming more aware of the cyber risks they face, but it's still not at an appropriate level.

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

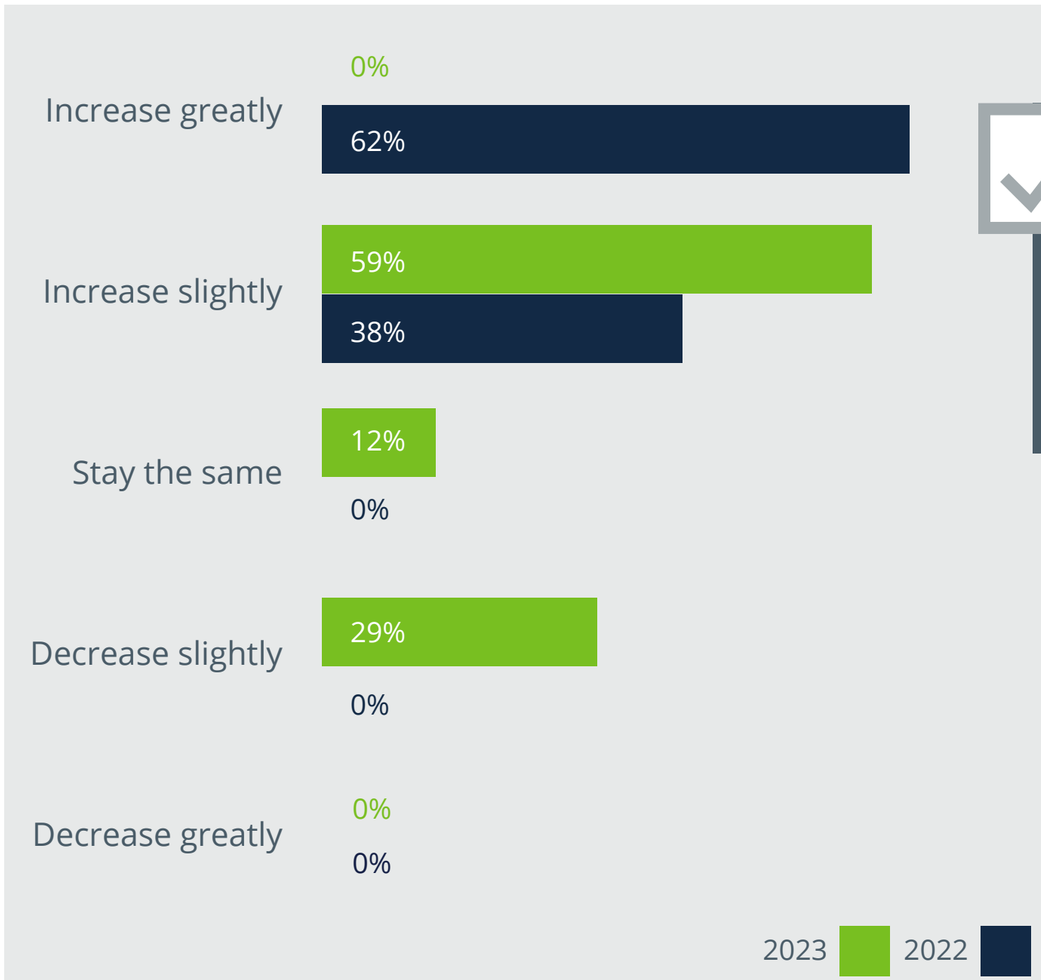


59% of underwriter believe companies should focus on **strengthening** their cybersecurity.

Underwriters continue to believe the number one risk mitigation strategy for companies in 2023 is focusing on improving security controls. As discussed in Section 1.1, however, the expected controls in place are a moving target.

Q5

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

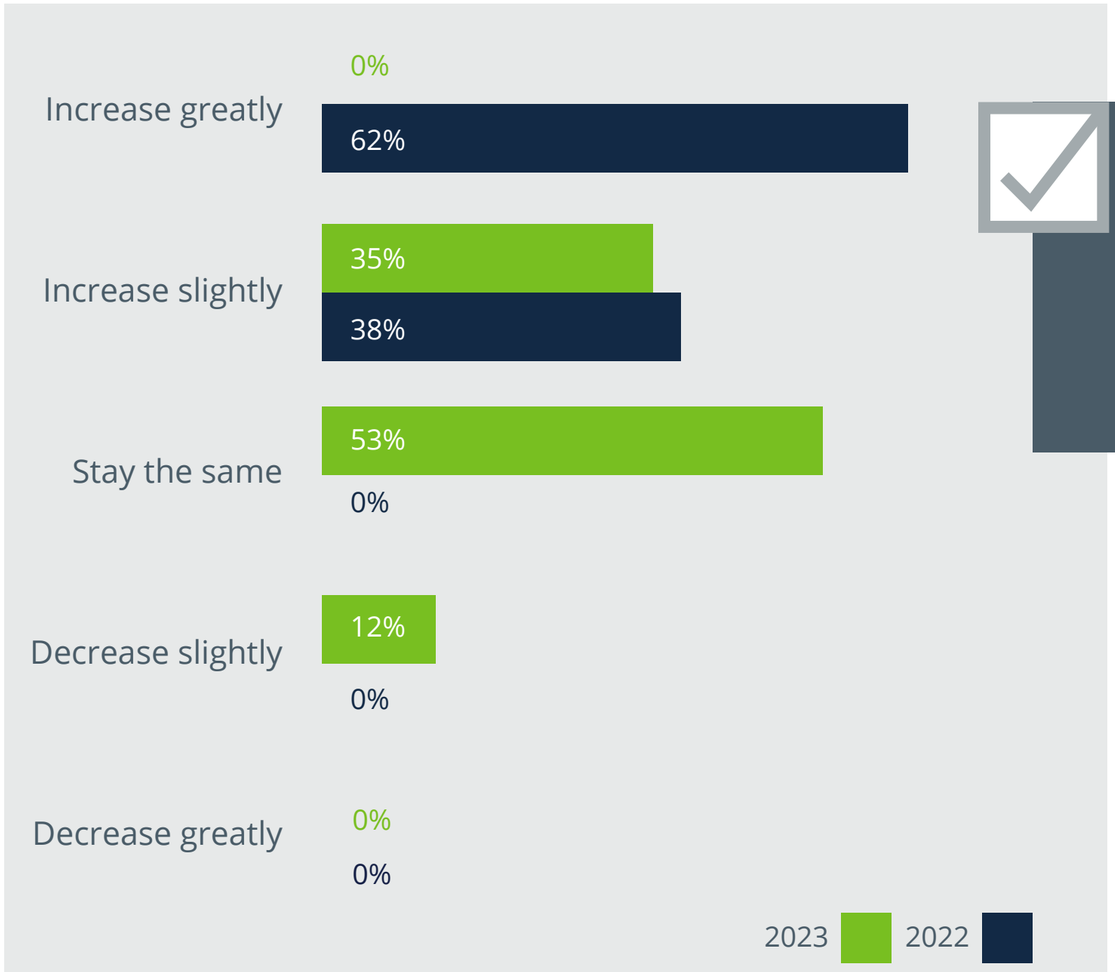


29% of underwriters believe cyber insurance **premiums** will **decrease** slightly.

The results here show the surest sign yet of a normalizing market—nearly 60-40 split between slight increase and stay the same/slight decrease. This is a significant improvement over underwriter attitudes on pricing one year ago.

Q6

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

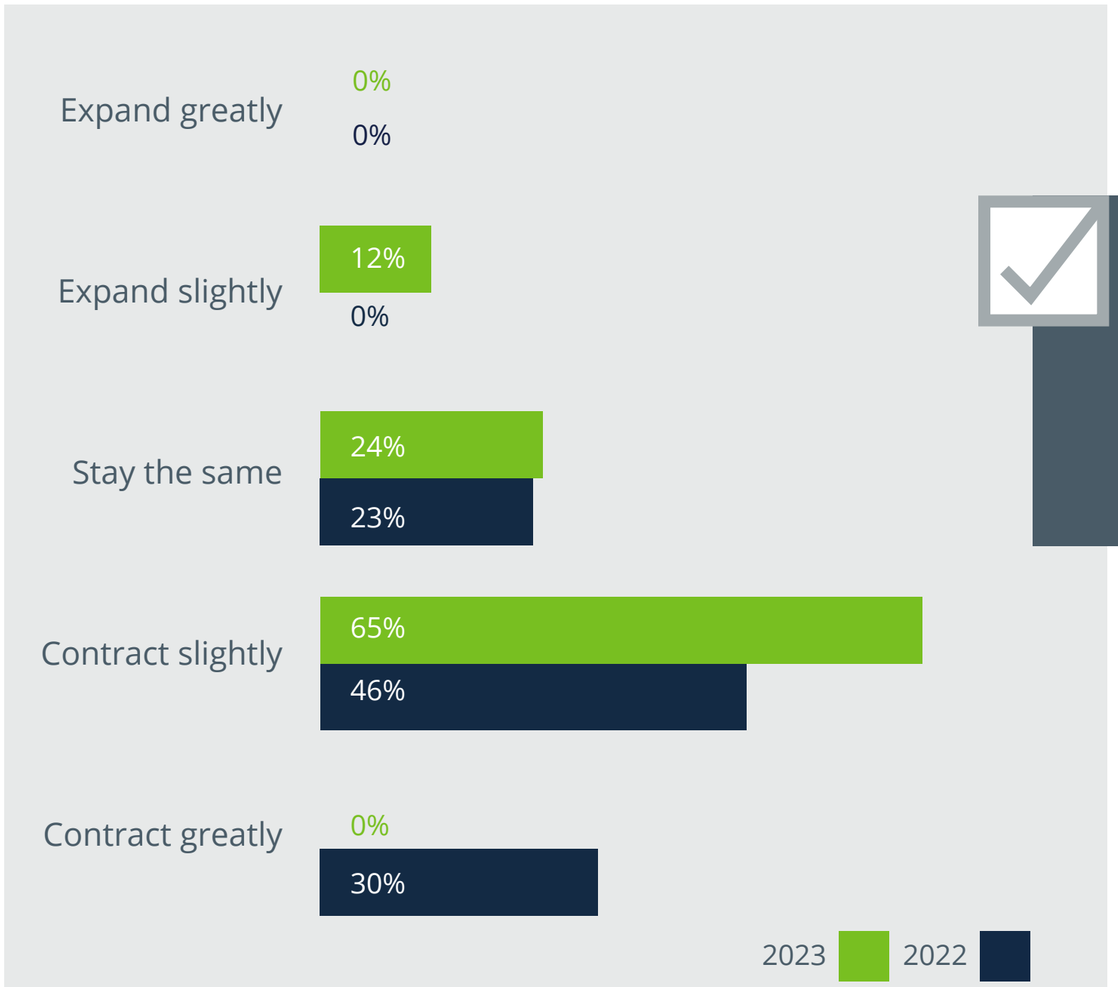


53% of underwriters expect **self-insured retentions to stay the same.**

The increased self-insured retentions (SIRs) we saw in 2022 have shown signs of stabilizing as we enter 2023. Underwriter sentiment suggests a slight uptick, but not near what we saw in 2022.

Q7

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



65% of respondents believe cyber policy **coverage** will **contract slightly.**

The area we expect most change in 2023 is contracted coverage. Look for changes specifically around systemic risk and coverage for privacy regulations.

In the next 12 months

100% of underwriters believe **cyber risk** will **increase** in 2023.

26% Greatly increase

74% Increase slightly

No. 1 threat companies face

53% of underwriters ranked **ransomware** as the number one threat.

29% Supply-chain attack

12% Privacy violation

Are companies sufficiently aware of cyber risk?

35% YES

65% NO

65% of insurers believe companies should be more aware of their cyber risk.

Risk mitigation strategy

59% Strengthening security

41% Improved processes and procedures

Future pricing

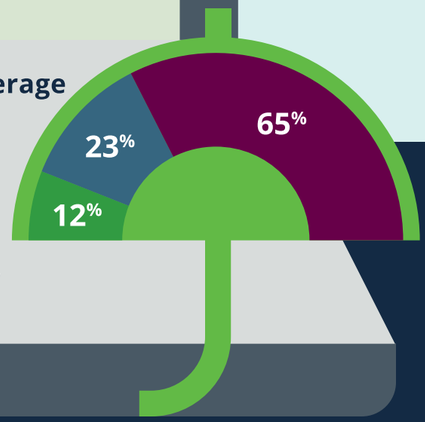
- Increase slightly
- Stay the same
- Decrease slightly

Cyber insurance premium

Cyber self-insured retentions

Cyper policy coverage

- Expand slightly
- Stay the same
- Contract slightly



4.0

Expert Insights

Priya Cherian Huskins
Senior Vice President, Management Liability

Stephen Quintana
Account Executive, Cyber/E&O/Media Liability

Lauri Floresca
Senior Vice President, Cyber Liability

Aaron Casey
AVP, Account Executive, Cyber/E&O/Media Liability

Keeley Sidow
Client Relationship Director, Management Liability

Start >>

4.1 Act Now to Prepare for the SEC's Cyber Rules

Priya Cherian Huskins

Senior Vice President,
Management Liability

Reach out to Priya >>

What do companies need to know about the SEC's proposed cyber rules?

The Securities and Exchange Commission (SEC) has been signaling for years that it has been unhappy about the way companies disclose cyber incidents. Now, it has proposed a set of rules that are intended to improve cyber governance, enhance cyber risk oversight, and drive more timely and specific cyber incident disclosures.

A version of the proposed rules will ultimately become final, so companies need to get ready now. At a minimum, this includes steps such as determining how your company will assess the financial impact of a cyber event and the efficacy of your disclosure committee. You don't want to wait until an actual incident to determine whether you will be able to respond as swiftly and thoroughly as the SEC requires. Waiting to take these steps could cause your moderately painful cyber incident to also become an excruciatingly painful D&O liability issue.

The SEC's New Proposed Cybersecurity Disclosures:
Next Steps for Boards of Directors

Read about the scope of the SEC's proposed rules and particular issues directors may want to consider in light of them.

Read Now >>

4.2 How to Get More Competitive Rates

Companies with deficient network security continue to see outsized premium increases and coverage restrictions. How should they approach the market to attract capacity and broad coverage at competitive rates?

Stephen Quintana

Account Executive,
Cyber/E&O/Media Liability

Reach out to Stephen >>

It's no surprise that "better risks" experience more favorable insurance pricing and terms. However, as the cyber market recovers from two years of significant loss activity, the divide between what companies with strong controls and those with lagging security can obtain in rates is quite substantial. Underwriting information is key, and there are a couple of steps insurance buyers should follow in this period of heightened underwriting rigor:

1. Start early. Scrambling right before renewal will be a burden on your team and can inhibit your ability to attract capacity in the market.
2. Engage the proper stakeholders at the firm (e.g., CISOs).
3. Elaborate on your network security strengths and highlight new processes/ tools on the roadmap for the next 12–18 months.
4. Determine areas of improvement and share the compensating controls you have in place.

A buyer's security controls will drive overall market interest but following the steps above to tell the story effectively can optimize results.

Cybersecurity Controls: Now Critical for Your Cyber Insurance Renewal

Many carriers will now decline cyber coverage for companies that don't meet the minimum baseline cybersecurity protections. Here's why and how you can get the best results when renewing your cyber insurance program.

Read Now >>

4.3 Standalone Cyber versus E&O Blended Policies

Why is it sometimes easier for non-tech companies to get cyber insurance than companies that specialize in technology? This seems counterintuitive.

Lauri Floresca

Senior Vice President,
Cyber Liability

Reach out to Lauri >>

Cyber insurance is sold in many forms, but for companies offering technology services, it's usually bundled with errors and omissions (E&O) coverage. Non-tech companies can buy standalone cyber policies (since they don't need the E&O coverage), and it's true that many more insurers are writing these policies. It would seem counterintuitive that technology companies have a harder time obtaining cyber insurance, since ransomware and phishing attacks are hitting a wide range of industries.

Insurers prefer to write standalone cyber because it doesn't have the added risk of that E&O component. They are worried about the aggregation of risk when a technology company becomes the vector for an attack to reach all its customers. In that case, what might have been a small breach can turn into a large E&O claim, with all those customers making demands to reimburse them for their financial losses.

The flip side, of course, is that technology companies often have better cybersecurity controls than those in industries like manufacturing, healthcare, retail, and professional services. When tech companies can document those strong controls, underwriters are more willing to offer coverage. Strong contractual protections and clear communication around shared security responsibilities between the vendor and its customers help, too. The good news is that with the cyber market showing signs of improvement, we expect more insurers to widen their appetite to include blended cyber/E&O in the near future.

4.4 Cyber Issues for FinTech

Aaron Casey

AVP, Account Executive,
Cyber/E&O/Media Liability

Reach out to Aaron>>

Do FinTech companies have different cyber risks, and how does this affect insurance?

Financial technology (FinTech) can be used to describe a wide range of companies. What traditionally might have described the computer technology used in the back office of banks or trading firms can now also describe neo-banks, payments apps, investment apps, or the blockchain. With this variety comes just as many exposures—like rapid growth in revenues, large record counts, technological disruption, and uncertainty due to regulatory changes.

In order to understand the nuances of risk across this broad category of companies, it's important for a FinTech company to understand how its revenue is generated. Companies selling to other businesses—B2B companies—will want to prioritize strong contractual protections in their contracts with customers to minimize their risk. Errors and omissions (E&O) insurance is important for this category.

Companies with greater exposure to consumers will want to focus on privacy and security controls—particularly in such a highly regulated industry. Regulators have placed greater emphasis on consumer protections and establishing best-in-class controls will help mitigate the risk of regulatory scrutiny.

There will certainly be nuance to the services being provided by FinTech companies, but the cyber risk faced by this industry rarely changes. FinTech companies are usually held to a higher standard of cybersecurity given the sensitive nature and volume of the information they collect, store, or process. Additionally, the critical nature of their operations means their availability and integrity are paramount to customer confidence.

4.5 Captives Will Continue to Expand

Keeley Sidow

Client Relationship Director, Management Liability

Reach out to Keeley>>

How has the hardened cyber market affected captive utilization in this area, and what do you expect going forward?

The tough market dynamics for cyber and technology E&O coverage over the last two years have certainly increased the number of companies thinking about alternative capital and unique program structures. It can be an important consideration but has proven to be most impactful for larger companies that have an existing, mature captive and are able to include cyber coverage within it. In this case, the captive capacity can be used strategically throughout a cyber program to maximize coverage and cost priorities.

Without an existing, well-funded captive in place, many companies have found the process too challenging—from both a timing and initial capital investment standpoint—to be worth it for cyber alone.

Going forward, we're optimistic that traditional insurance capacity will be more available than it has been over the last two years for cyber and technology E&O. In addition, while captive utilization and other alternative capital will continue to develop and expand, it will be less out of necessity to achieve desired coverage results and more related to a company's overall strategic approach to enterprise risk transfer.

Captive Insurance as a Solution for the Tough Cyber Market

Learn what a captive insurer is, how captives can be used for cyber insurance, the challenges in using a cyber captive, and the option of adding cyber insurance to a mature captive.

Read Now >>

5.0

Concluding Perspective

Carolyn Polikoff
President of Commercial Lines

Start >>

We're happy to report a normalizing cyber insurance market and the easing of price increases for 2023 in our second annual *Cyber Looking Ahead Guide*. After a couple of volatile years, with significant premium hikes for many buyers, this is welcome news.

Carolyn Polikoff
President of Commercial Lines
Reach out to Carolyn>>

Our *Guide* details the trends impacting the industry and explains these pricing updates and the reasons behind them. While things are getting better, the cyber industry still faces many challenges. Systemic risk is a major issue, and technology errors & omissions (E&O) insurance remains difficult. The C-suite continues to be held liable for cybersecurity failures, and California's new consumer privacy law took effect this year.

Our Underwriters' Survey reinforces the notion of a normalizing market, and respondents are much more optimistic about pricing than they were last year. But underwriters continue to say that ransomware is still the biggest cyber threat companies face and that companies need to be more aware of their cyber risks.

Like in our previous *Guide*, we recommend buyers focus on their security controls to reduce their risk. Yesterday's standard security practices are no match for today's data breaches, network failures, cyber extortion, and other sophisticated cybercrimes.

Woodruff Sawyer helps safeguard against the constantly evolving web of cyber liability exposures that all industries face today. Our expertise and experience in this specialty line allow us to leverage data for our clients' benefit—enabling them to make informed decisions about their cyber risk management strategy and insurance programs. If you have questions about mitigating and transferring cyber risk, our experts are here to answer them.

About Woodruff Sawyer

As one of the largest 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.

woodruffsawyer.com

Find out why clients choose to work with Woodruff Sawyer.

Subscribe for Expert Advice and Insights

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

Additional Resources

The Cyber Notebook >>

The D&O Notebook >>

Woodruff Sawyer Insights >>

Woodruff Sawyer Events >>

Watch Dan Burke's video insights into hot topics in cyber liability >>