WOODRUFF SAWYER

CYBER LIABILITY

Looking Ahead to 2022

CYBER INSURANCE EXPECTATIONS FOR THE COMING YEAR

TABLE OF CONTENTS

1.0 CYBER MARKET UPDATE

Dan Burke

Senior Vice President,
National Cyber
Practice Leader

REACH OUT TO DAN >

Return to Table of Contents >>

1.1 US Market Update

To call 2021 anything other than a sea change in the cyber insurance world would be an understatement. Indeed, nearly all cyber insurance renewals saw increases in premium and self-insured retentions throughout 2021. Many saw reductions in limits. Everyone experienced the increased scrutiny of cybersecurity controls to combat ransomware. According to this year's Underwriters' Survey, 2022 doesn't hold much relief. Let's dive deeper into the trends we've seen throughout 2021 and what they signal for 2022.

The Hard Market Arrived with a Vengeance

While 2020 showed signs of a hardening market, the acceleration of difficult conditions throughout 2021 is unprecedented in the history of cyber insurance. Reinsurance treaty renewals in January of 2021 forebode the changing conditions in the primary cyber insurance market, and ransomware is the main concern. Indeed, as you'll read in the **Hot Topics section 2.1**, a dramatic rise in ransomware claim frequency and severity led to sharp reactions from the cyber insurance market.

Technology Errors and Omissions (E&O) Aggregation Concerns

Aggregation risk concerns have dominated the conversation around technology errors and omissions risk. Many SaaS platforms and, in particular, security software providers have seen steep increases in premiums—with little weight given to any strong security controls in place. It's also easy to see the impact of COVID-19 and remote work in this space. Just as most companies are relying more on technology, and software companies are seeing explosive growth, the insurance market views their risk as even greater than before.

Multi-Factor Authentication: A Small Step for a Big Decline in Cyber Attacks >>

Multi-factor authentication (MFA) is an increasingly important solution to thwart account compromise attacks, especially when the workforce is remote and gaining access to key corporate networks and applications is vital.

Rise of Cyber MGAs and InsureTech

It's not all bad news within the cyber insurance market, as a number of technology-forward cyber **managing general agents** (MGAs) have burst onto the scene over the last few years. Initially focused on small business risks, many of these MGAs have hit an inflection point and are beginning to focus on more medium-to-large sized risks. This has the potential to provide needed capacity support for larger insurance programs, although the progress here is still minimal. Greater adoption of MGA capacity and the

willingness of traditional cyber insurance carriers to write insurance above these MGAs in a cyber insurance tower will be an area to watch throughout 2022.

> A Managing General Agent (MGA) is a specialized type of insurance broker who is vested with underwriting authority from an insurer.

1.2 Pricing Trends

The surest sign of a hard cyber insurance market has been the increase in pricing for companies of all sizes, in all sectors. The Woodruff Sawyer Cyber Pricing Index shows the change in pricing at the median and top quartile during a trailing 12-month period over the past year for both primary and excess prices.

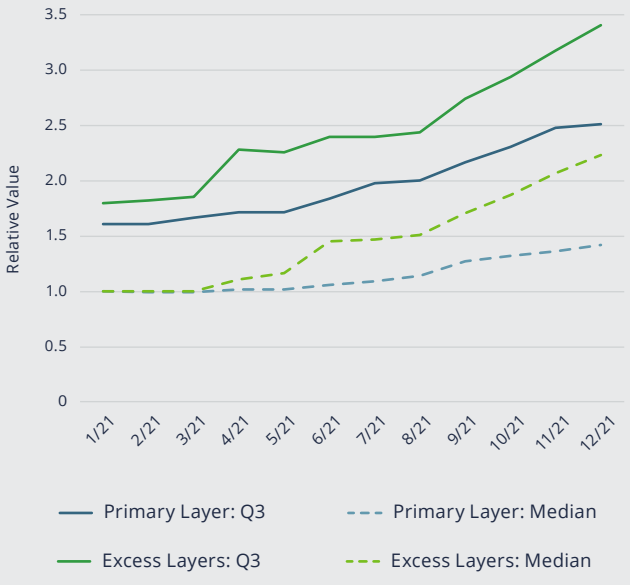
One of the hallmarks of a hard insurance market is present in the data—that excess pricing has deteriorated sooner and more rapidly than primary pricing. With the median excess insurance price up 123% since the previous year, the impact on overall insurance premiums is most realized for companies that buy high limits.

Another key takeaway is the impact of pricing changes at the top quartile as compared to the median. A hard insurance market doesn't hit all companies in the same way, and indeed the data shows that those who pay the highest premiums have seen higher percentage increases year over year than those near the median or bottom quartile of pricing. A year ago, the top quartile premiums were about 61% higher than the median, and today that number is 109% higher than the median—an increase of 79%.

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 Insurance Pricing Continued to Deteriorate Throughout 2021, Ending at High Watermarks for the Past 12 Months

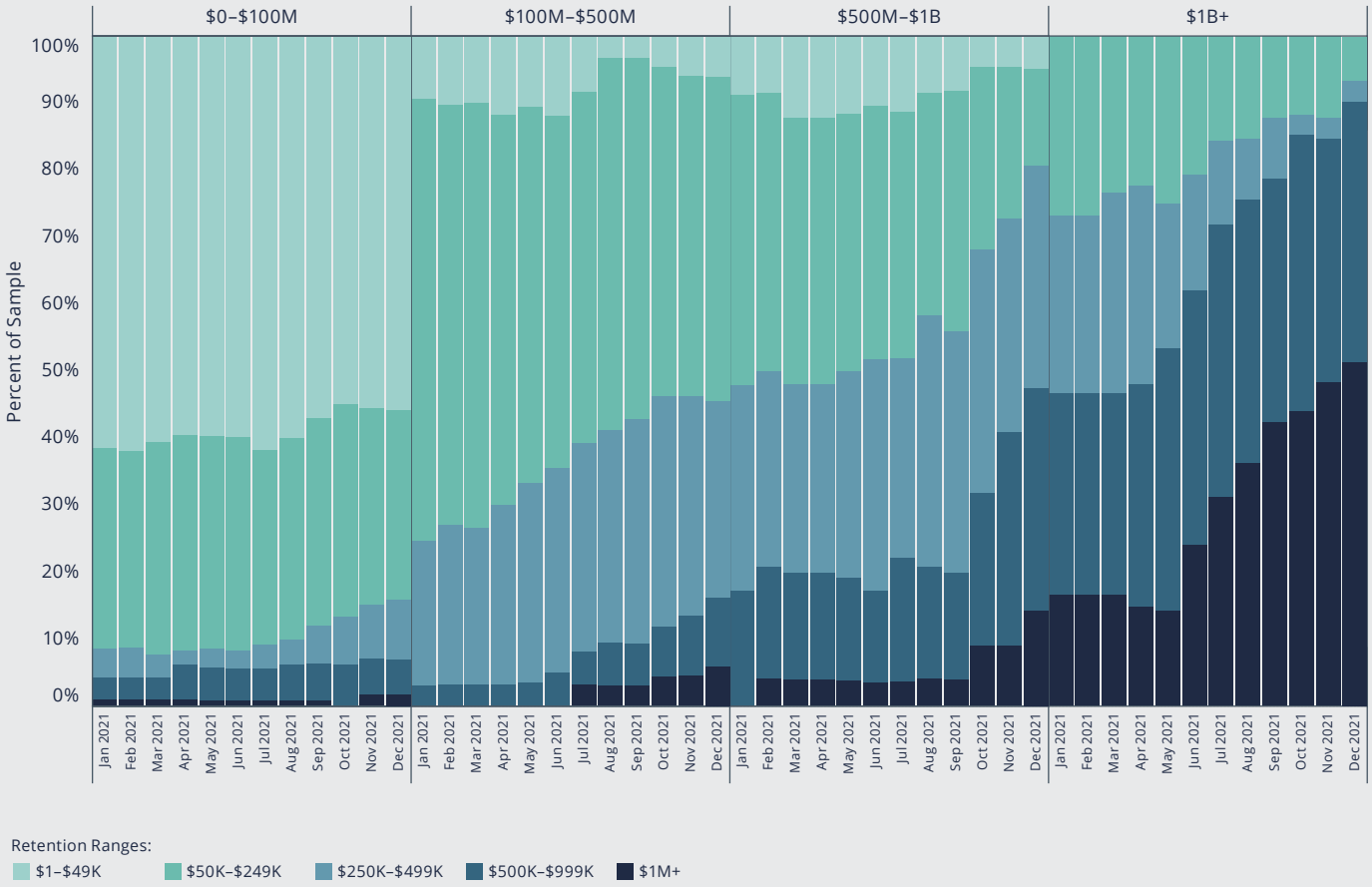


1.3 Self-Insured Retention Trends

Insurance carriers view cyber risk as on the rise. As a result, they've not only increased premiums but they've also asked companies to keep more risk on their balance sheet in the form of self-insured retention increases. Across companies of all sizes, Woodruff Sawyer clients have seen retention increases over the past 12 months.

Companies in Every Revenue Segment Have Seen Increases in Self-Insured Retentions Over the Last 12 Months

Self-Insured Retention Trend by Company's Annual Revenue



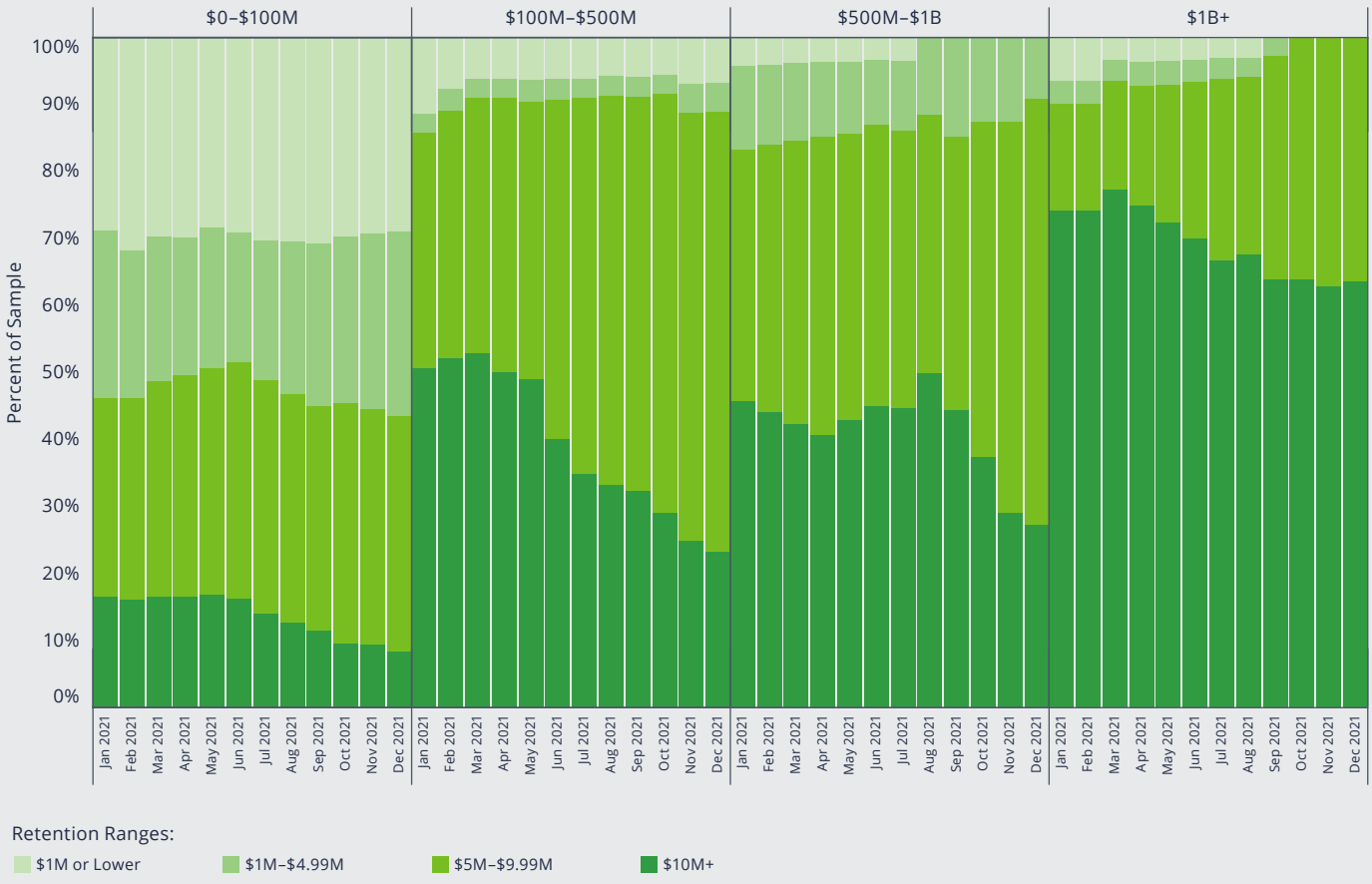
1.4 Limit Trends

Another concerning trend for companies looking to purchase high cyber limits is the change in primary limit profile that we've seen across the last 12 months. A restriction of available capacity is common during a hard market, and in the cyber insurance market we've seen many carriers reduce their available capacity throughout 2021 to a maximum of $5 million for any one client.

This is most pronounced in the middle-market revenue segment of $100 million–$500 million in revenue, where the share of companies with a $10 million primary limit has plummeted, and the share of companies with a $5 million primary limit has made up the difference.

In the Cyber Insurance Market, We've Seen Many Carriers Reduce Their Available Capacity Throughout 2021 to a Maximum of $5 Million for Any One Client

Primary Limit Purchase Trend by Company's Annual Revenue



2.0 HOT TOPICS

Return to Table of Contents >>

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 facing companies today.

2.1 Ransomware

It's hard to talk about cyber risk these days without hearing about the threat of ransomware. The federal government, security experts, and insurance underwriters alike are intensely focused on the rise of ransomware attacks and their increasingly costly recovery process.

Ransomware attacks were expected to occur every **11 seconds** in 2021 and proved costly to companies that were impacted.[1]

The average ransom payment has grown **82%** from 2020 to 2021. The news is increasingly filled with ransom demands in the tens of millions of dollars.[2]

Yet the amount of ransom demanded is not always the most expensive part of a ransomware attack. Cyber insurance provides support to companies impacted by ransomware by providing access to experts who can help a company respond—think lawyers, IT forensic specialists, and ransom negotiators. The fees charged by these experts can add up quickly.

However, we hear repeatedly from insurance carriers that the biggest cost of a ransomware attack is the business interruption losses incurred while the affected network is down. According to Coveware, the average downtime that companies experience during a ransomware attack is 21 days. The lost profits and fixed expenses incurred during this downtime are recoverable under insurance—and that is proving to be one of the most valuable aspects of having cyber insurance.

Three Things to Consider Before Paying the Ransom from a Ransomware Attack >>

Get the answer to the question on the minds of many CISOs and company executives: If we are the victim of a cyber attack, should we pay the ransom?

1. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021
2. **https://www.darkreading.com/attacks-breaches/average-ransomware-payment-hits-570000-in-h1-2021**

Minimum Protection	Baseline Protection	Best Protection
Email Security • Email tagging • Email content and delivery – sender policy framework (SPF) checks • Office 365 add-ons and configuration **Backup and Recovery Policies** • Back up key systems and databases **Internal Security** • Deploy and maintain a well-configured and centrally managed antivirus solution • Macros: limit use • Patching cadence • Well-defined and rehearsed incident response process • Educate your users (phishing training, etc.) • Manage access effectively (i.e., MFA, privileged access)	**Backup and Recovery Policies** • Regular testing of backups • Disconnect backups from organization's network • Separately stored, unique backup credentials **Internal Security** • Establish a secure baseline configuration • Filter web browsing traffic • Use of protective DNS • End-point detection and response (EDR) tools	**Backup and Recovery Policies** • Encrypted backups **Internal Security** • Comprehensive centralized log monitoring • Subscription to external threat intelligence services • Network segregation (i.e., via access control or well-configured firewall

As ransomware severity and frequency continues to rise, cyber insurers have now started requesting additional underwriting information around defenses they expect companies to have implemented to protect themselves from a ransomware event.

Identity Management and Privileged Access Controls: Important but Often Overlooked in Cybersecurity >>

Read more for insight into how you can keep hackers from taking total remote control of your systems.

2.2 Supply Chain Attacks

If the conversation around ransomware hasn't taken all the oxygen out of the room yet, then the uptick in supply chain attacks may do the trick. Specifically for technology companies, 2021 brought to bear a number of attacks against security software tools that had far-reaching impacts throughout the technology supply chain.

Companies like SolarWinds, Microsoft, and Kaseya faced sophisticated attacks that exposed vulnerabilities in their products, which were used by thousands of customers. In two different ways, these attacks highlighted a significant concern of the cyber insurance industry—aggregation risk.

By infiltrating the products that were ultimately distributed to thousands of customers, the attackers created the ability to deploy their malware at each downstream end-user and multiply the number of targets for their attack. Insurance carriers have highlighted this aggregation of risk—potentially all the customers of a single company having cyber incidents at one time—as a significant source of concern.

Viewed another way, this aggregation risk actually becomes a source of great errors and omissions (E&O) risk for the technology companies that provide the compromised products. Typically, contractual provisions will limit the amount of risk a technology provider may face due to the failure of their product, and E&O insurance is purchased to respond to an individual client's problems. However, when that product failure is a result of a cybersecurity failure, the risk of a client suffering damages is amplified by the number of clients impacted.

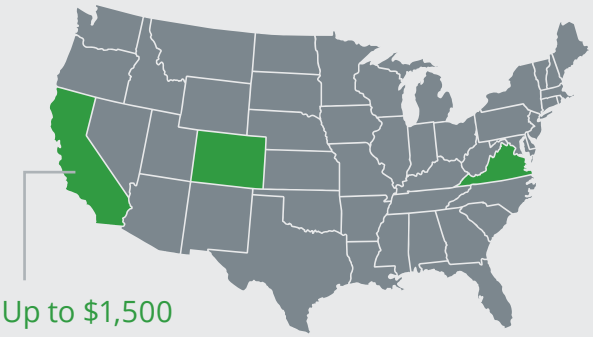
The efficiency of these attacks against the technology supply chain throughout 2021 suggest that similar attacks may be on the horizon in 2022.

Cyber Security Controls: Now Critical for Your Cyber Insurance Renewal >>

Implement a cyber security control or you might not be able to get cyber insurance at all.

2.3 Privacy Regulation Changes

The implementation of the European Union's General Data Protection Regulation (GDPR) in 2018 has ushered in a wave of consumer privacy rights regulations across the globe, each law attempting to further the rights of consumers over the collection and processing of their data. For companies that provide a consumer-facing product or service, there may be no greater organizational risk than that of complying with these various privacy laws.



Up to $1,500 per record breached

Myriad state laws throughout the United States have begun to get passed by legislatures, specifically in California, Colorado, and Virginia. A key element of these state consumer privacy laws is the private right of action—a grant that provides consumers with the damages defined in the law for a data breach. In California, for example, these private right of action damages can be up to $1,500 per record breached.

There is precedent for these private rights of action being levied against companies for failing to appropriately disclose collection, processing, storage, and use of data. The Illinois Biometric Information Law includes a private right of action and has led to significant settlements from companies that find themselves sued under the law.

And then there are international laws that carry even further penalties—sometimes holding executives of a company personally liable for damages, such as China's Personal Information Protection Law (PIPL). This law went into effect in November 2021 and includes potential fines against individuals, as well as fines against violating companies.

Under many of these privacy laws, we have yet to see significant movement on the volume of cases brought under the laws. Such limited data on settlements makes it hard to predict the actual impact companies may face for alleged non-compliance with the laws, but the potential for a significant settlement remains a key risk for consumer-facing companies.

The BIPA Litigation Landscape and What Lies Ahead >>

Class action litigation for non-breach privacy violations has exploded, and the Illinois Biometric Information Privacy Act (BIPA) is the culprit.

2.4 Mass Arbitration

Sticking with key risks for consumer-facing companies, the threat of mass arbitration events looms large for 2022. For years, a common practice was for companies to include mandatory arbitration provisions in their click-through user agreements. Consumers would agree to standard terms of service to get access to the product and not read the fine print. This tactic was considered to be a class action prevention tool, forcing

consumers to individually arbitrate their claims against a company rather than group together as a class.

Recently, plaintiff firms have been calling the bluff of companies that deployed this tactic. They've been filing individual arbitration demands for thousands of customers against a single company and holding the company to the terms of their own contracts where they agree to pay the filing fees. All told, the filing fees alone can cost tens of millions of dollars.

Mandatory arbitration doesn't look as appealing when the fees get that large.

This risk is still relatively new and, to date, has really only impacted some of the largest name brands in consumer goods and services. The first mass arbitration cases appeared in 2018, but they've gained notoriety for their effectiveness, and several court decisions have held to task the companies that demanded the arbitration.

2.5 Federal Government Intervention in Cyber Security

The United States government has also taken note of the increasing amount of cyber risk faced by private sector companies—and their actions are having impacts on the risk of companies across many sectors.

Much of the focus of the US government to date has been on ransomware, which is reasonable given the change in risk noted above. They've approached this risk from a couple of angles: sanctions and reporting requirements.

In 2020, the US Department of the Treasury came out with updated guidance for companies paying ransoms to individuals or entities on the Office of Foreign Asset Control sanction list. Notably, they affirmed an expanded number of companies that could potentially be subject to penalties for a payment made to a sanctioned entity, including any firm that supported a company in making the illegal payment. Insurance carriers, law firms, banks, and IT forensic providers were now all subject to the same penalties as the ransomed company, putting more pressure on these firms when dealing with a ransomware response.

The Department of the Treasury has also been active in adding many more individuals and specific ransomware gangs to the list of sanctioned entities. They've even taken note of cryptocurrency exchanges, which have long been used by ransomware gangs to launder the cryptocurrency used to pay ransoms.

> The Department of the Treasury is taking note of cryptocurrency exchanges, which ransomware gangs use to launder their ransoms.

Finally, there has been movement toward passing a cyber event reporting law. The specific details of the law are yet to be determined, but current expectations will require reporting of a successful cybersecurity attack to a government entity—likely either CISA or the FBI—for companies in the critical infrastructure or government contractor sectors. We expect that the requirements imposed on these two sectors will quickly make their way deeper into the private sector and impact nearly all companies.

Should We Call the FBI After Our Cyber Incident? The Surprising Benefits >>

Key benefits exist to engaging authorities like the FBI when the cyber incident calls for it. Let's look in more detail at when and why you'd call the FBI.

2.6 The War Exclusion and Nation-State Sponsored Hacking

In November 2021, the Lloyd's Market Association—a membership group representing all syndicates at Lloyd's of London—**issued guidance** for their members regarding the application of the war exclusion to standalone cyber insurance policies in the event of nation-state-sponsored hacking events.

The guidance makes it clear that underwriters should not be providing coverage for attacks from nation-state government actors against the private sector. There are a number of details yet to be determined as to how this guidance will actually be implemented and its impact on the cyber insurance market overall—but this is a development worth watching.

To date, we have not seen cyber insurance claims denied due to the invocation of the war exclusion—even when the attackers are alleged to be sponsored or supported by foreign governments. The primary examples of this exclusion being applied come from a cyber loss reported to a property insurance policy, not a standalone cyber insurance policy.

State-Sponsored Cyber Attacks and the War Exclusion: Are You Covered? >>

In April 2021, the Biden executive order sanctioning Russia for the Solar Winds attack led to a lot of questions about the impact on the war exclusion of a cyber insurance policy.

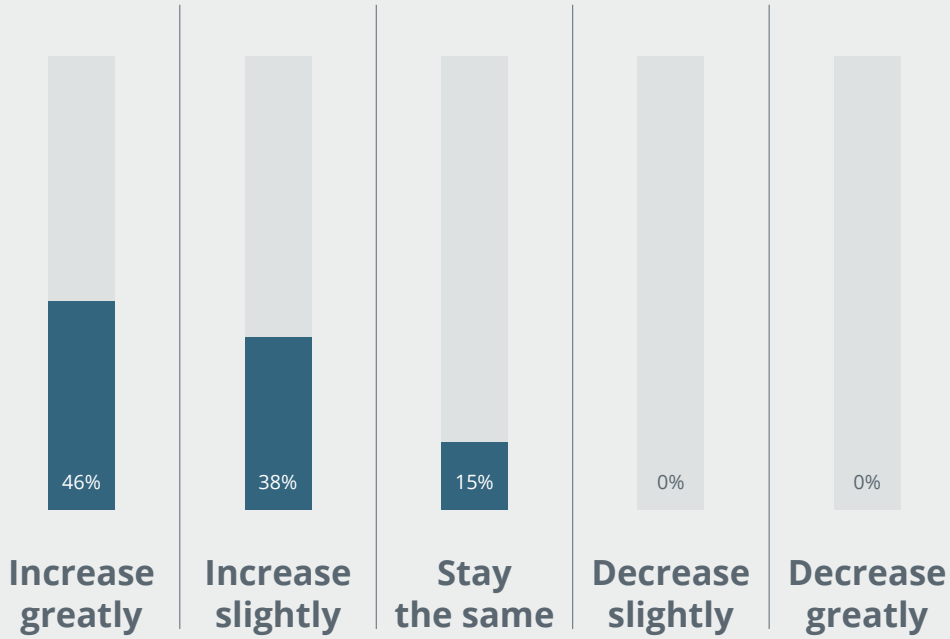
3.0 UNDERWRITERS' SURVEY

Return to Table of Contents >>

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 view of the world, including their current appetite for risk. Woodruff Sawyer is in conversation with insurance carriers every day. For this section of *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 2022. Let's dive in.

Q1 Over the next 12 months, will cyber risk:



2021 SURVEY RESULTS

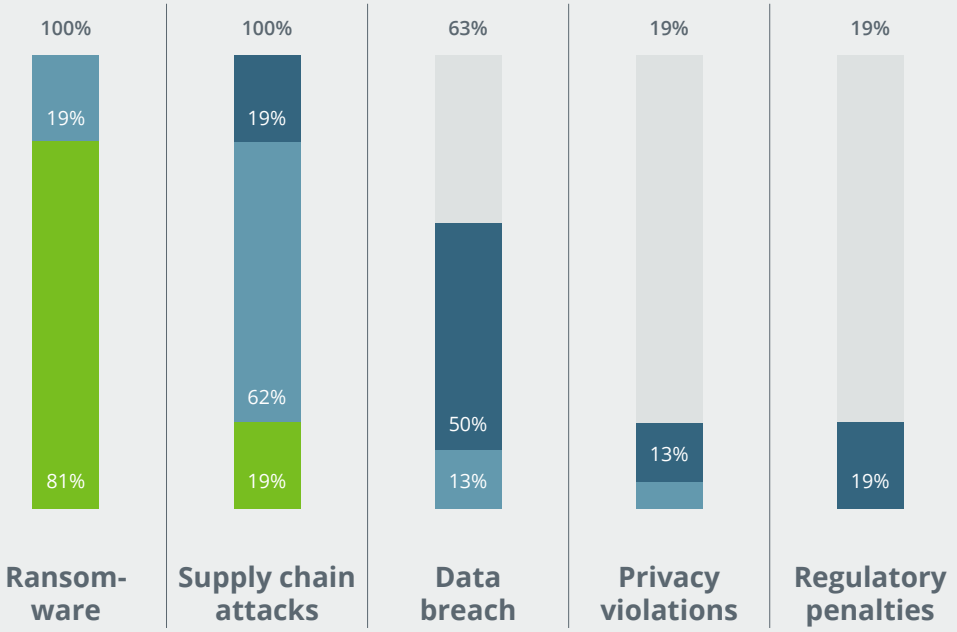
46%

of underwriters believe cyber risk will increase greatly in 2022

A

Underwriters are in near-universal agreement: cyber risk is increasing across the board. Interestingly, nearly half of the underwriters surveyed believe cyber risk will increase greatly in the next year. None believe that companies will face less cyber risk.

Q2 What is the most concerning threat companies face?



2021 SURVEY RESULTS

100%

of underwriters ranked ransomware and supply chain attacks among their top three threats

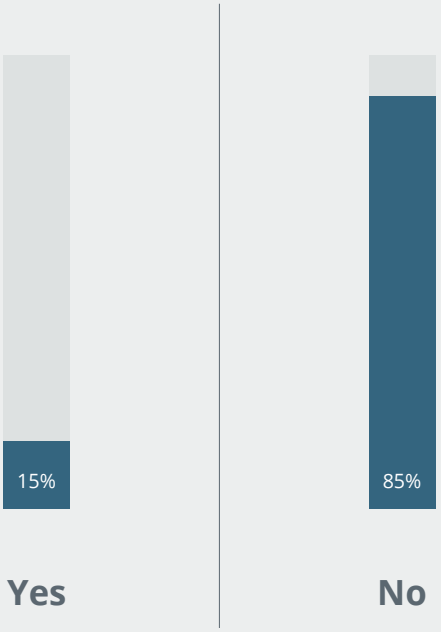
Ranked 1st 2nd 3rd

A

Privacy violations ranked as a low concern for most underwriters despite an increase in global regulations around consumer privacy rights.

When asked to list additional threats that concern them, underwriters mentioned cloud outages, catastrophic events, destructive malware, targeted attacks intended to cause bodily injury or property damage, and aggregation of risk at single points of failure.

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



2021 SURVEY RESULTS

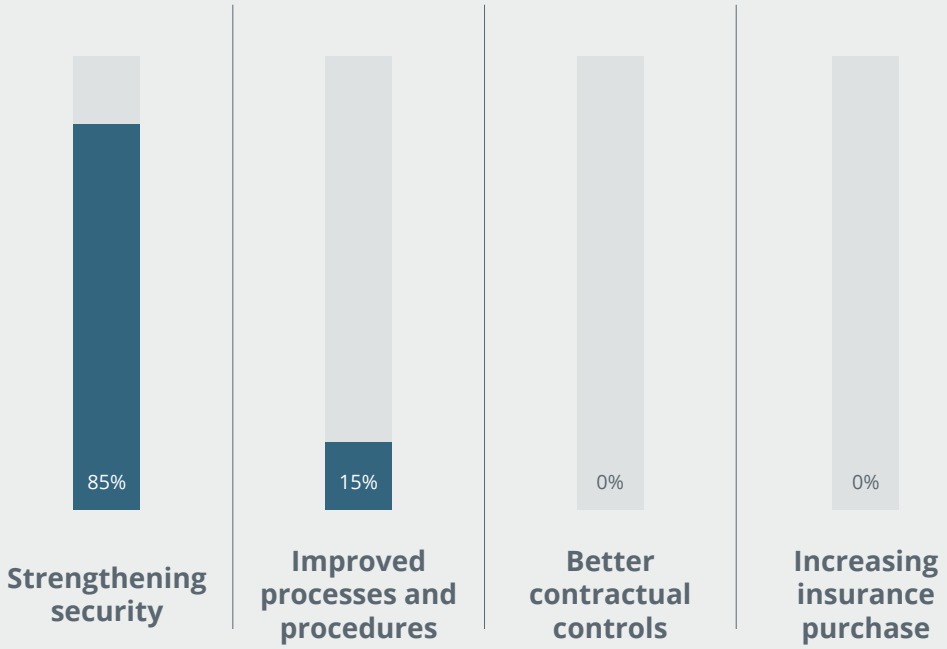
85%

of insurers believe companies should be more aware of their cyber risk

A

It is almost universally agreed that companies should be more aware of the cyber risk they face. While this is not a surprising data point on its own, considering that cyber insurance underwriters live in the world of cyber risk every day, it does point to a difference in the value attributed to the risk by underwriters, which is reflected in the price changes discussed in section 1.2.

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



2021 SURVEY RESULTS

85%

of underwriters believe companies should focus on strengthening their cyber security

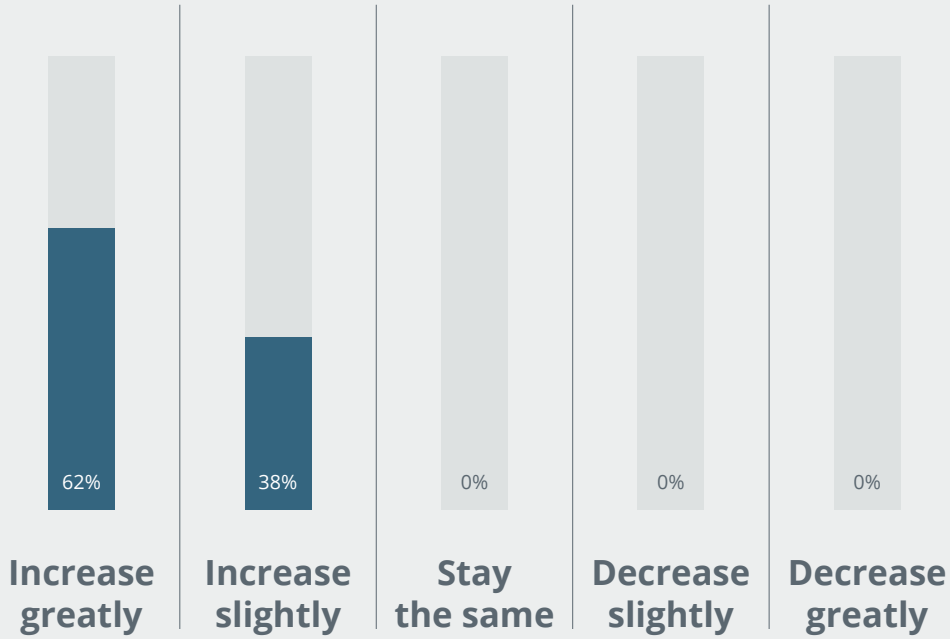
A

As discussed in section 4.4, companies today are facing a much more intense underwriting process, with a high level of scrutiny on security controls and internal processes and procedures around cyber risk. It is no coincidence that underwriters believe these two areas need the most focus over the next 12 months.

We also note that no underwriters thought that companies should be purchasing higher limits to mitigate their risk. This may point to their preference for reduced capacity, discussed in section 1.4.

Q5

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



2021 SURVEY RESULTS

62%

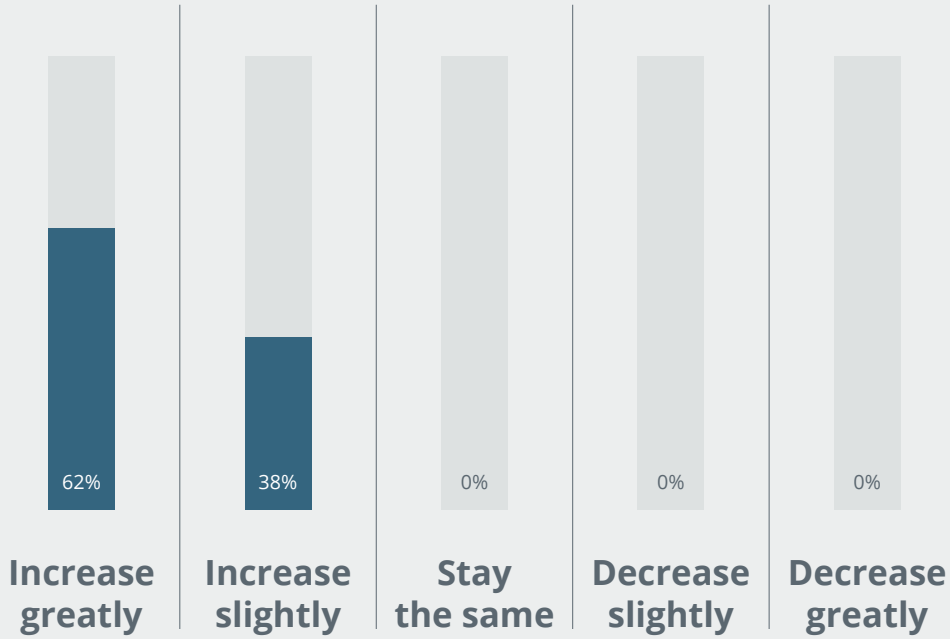
of underwriters believe cyber insurance premiums will greatly increase

A

It's clear to see that the pricing increases noted in section 1.2 are going to continue into 2022. Over 60% of our respondents expect prices to increase greatly over the next 12 months, while none foresee a decrease in cyber insurance premiums.

Q6

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



2021 SURVEY RESULTS

62%

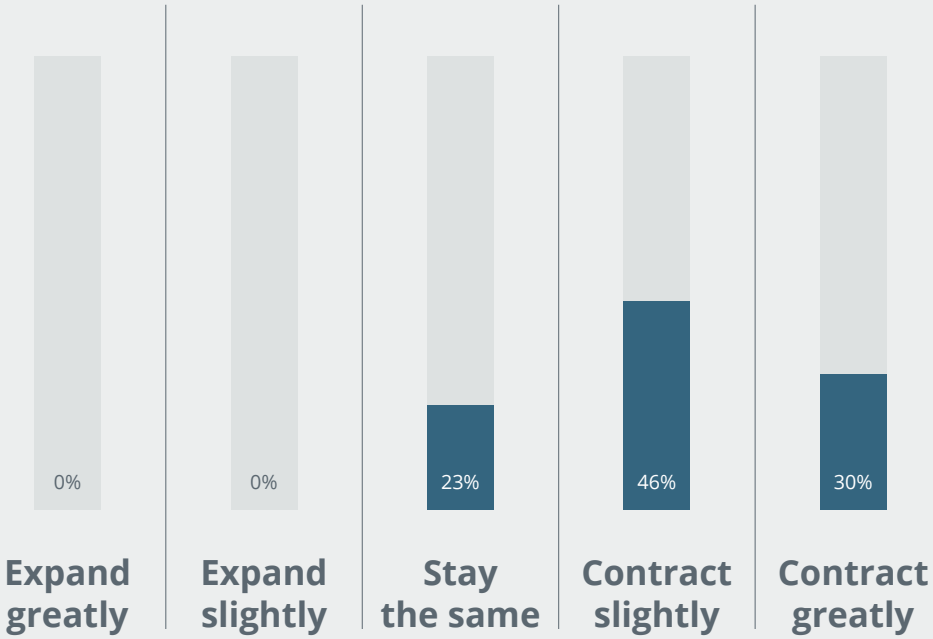
of underwriters expect self-insured retentions to increase

A

Similar to the premium question asked above, cyber insurance underwriters expect self-insured retentions to increase through 2022 as well. Expect the trend lines identified in section 1.3 to continue their upward trajectory.

Q7

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



2021 SURVEY RESULTS

46%

of respondents believe cyber policy coverage will contract slightly

A

Cyber insurance policies have greatly expanded coverage over the last 5-10 years, although that began to change in 2021. Underwriters expect more contraction of policy coverage next year, although the results suggest a more tempered change compared to what you should expect for premiums and self-insured retentions. Nearly 75% of the respondents expect coverage to stay the same or contract only slightly.

4.0 EXPERT INSIGHTS

Return to Table of Contents >>

Lauri Floresca

Senior Vice President,
Cyber Liability

REACH OUT TO LAURI >

READ NOW >

Cyber 101: Understand the Basics of Cyber Liability Insurance

Every company has cyber risk. Get started with the basics of cyber liability insurance to help your company manage this risk and protect your business now.

4.1 Forget Everything You Know About Cyber Limits

Q. Cyber risk is harder to insure and yet more prominent than ever. How do we get creative in transferring our risk?

A. With the cyber market in turmoil, companies are being forced to reassess the size and structure of what they are buying. Maybe that's a good thing.

Over the last 10 years, the cyber insurance market has expanded to combine many different types of coverage in one contract. When cyber insurance was cheap and easy to get, this bundled approach made purchasing coverage efficient. Now it is driving up costs and limiting capacity. Some insurers aren't comfortable offering technology E&O. Others are not writing cyber business interruption. Others are limiting media coverage. Knowing what you want and need before you go into the renewal market can help focus your efforts.

Many companies buy at least a minimum amount of coverage to satisfy contractual requirements. Beyond that, it is important to understand your actual risk profile. With our partner Cyber Cube, we help our clients model the potential impacts of different cyber events, including a data breach, network impairment, or ransomware event.

Where coverage has become more difficult to obtain, some clients are choosing to self-insure more aspects of cyber. This can be tricky where you have contractual requirements, but in many cases a fronted policy can be a solution.

The challenging market for cyber insurance is forcing creativity—which might be for the best in the long run.

Priya Cherian Huskins

Senior Vice President,
Management Liability

REACH OUT TO PRIYA >

READ NOW >

Cybersecurity Controls and Procedures: Lessons Learned from the SEC's Latest Enforcement Action

Read more about the SEC standards and establishing cybersecurity and cyber reporting policies and procedures.

Is Your Board Prepared for the Growing Risk of Ransomware Attacks?

Learn some practical ways boards can prepare for a ransomware attack.

4.2 Cyber Risk for Boards

Q. What do boards of directors need to know when it comes to cyber risk?

A. First and foremost, boards are responsible for cyber risk oversight from a fiduciary duty perspective, and the SEC has made it clear that it expects disclosures concerning cyber risk to be accurate. The good news is that the law doesn't require that boards get everything right, only that boards make a reasonable effort. This means setting up systems that are designed to bring important risks to the board's attention and then acting on this information. It also means taking a proactive approach to assessing risks. For example, boards will want to take an especially thoughtful approach to dealing with ransomware.

Evan Hessel

Casualty Practice Leader

REACH OUT TO EVAN >

READ NOW >

Captive Insurance as a Solution for the Tough Cyber Market

Read more for insight into captives, insurers, the caveats, and the benefits of captives for cyber insurance.

4.3 Captive Insurance: A Solution for a Tough Cyber Market

Q. How can a captive be used to finance our cyber risk?

A. Unfortunately, starting a captive insurer for the primary purpose of insuring cyber liability is unlikely to be a cost-effective replacement for commercial cyber insurance. Forming a captive is not a cheap or simple transaction. Captives require substantive strategic resources, regulatory capital, and operational costs—all of which, in total, often make traditional cyber insurance look like a smart purchase (even at higher premiums).

One caveat to this analysis: for large organizations with well-established captives that hold significant underwriting surplus generated from other coverages, adding cyber liability may be a sensible potential strategy to mitigate the impact of a hardened cyber market.

Robin Fischer

Senior Vice President,
Risk Management &
Cyber Liability

REACH OUT TO ROBIN >

READ NOW >

Cyber Insurance Underwriting Is Changing

Cyber insurers are tightening underwriting guidelines and clarifying policy language. Learn what to keep in mind as you purchase cyber insurance for the first time or renew your policy.

Ransomware Attacks Continue to Cause More Underwriter Scrutiny

Given the increase in claims from recent ransomware attacks, cyber insurers are requiring even more information as part of their underwriting processes.

4.4 Handling the Intense Underwriting Process in 2022

Q. How can cyber buyers ensure a better outcome in 2022?

A. In order to achieve a better outcome in today's cyber insurance placement or renewal, invest more time into the process.

Expect underwriters to want to review information about your basic exposures, information security controls, data backup procedures, regulatory compliance, and company policies and procedures. In addition, many carriers are now requiring supplemental applications documenting specific controls for ransomware, dependent business interruption recovery procedures, and operational technology networks.

To prepare for this increased level of scrutiny, make sure your teams are ready, including the legal, finance, and security teams. Gather your information, review it for areas that might lack some controls, and be prepared to discuss a remediation plan to get your company up to speed. It's also a good idea to highlight the areas where you've made improvements over the past year to show your commitment to good cybersecurity practices.

One last recommendation is to start early. Aim for 90 to 120 days ahead of the renewal or inception date. When in doubt, ask your broker.

Jesse Attix

Senior Vice President,
Management Liability

REACH OUT TO JESSE >

READ NOW >

Nail Your Communications During a Cyber Event

Read more for the three things you should consider as you forge a communications strategy as part of your cyber incident response plan.

4.5 Effective Breach Response Process

Q. How can a company best prepare an effective breach response process?

A. Being properly prepared to respond to a cyber event is fundamental to every company's success. This starts with a documented incident response plan.

Almost every cyber event will require the engagement of breach/privacy counsel to provide guidance on legal/regulatory obligations that arise from a breach—notification to individuals when PII or PHI is exposed, communication to state attorneys general, compliance with international laws, etc.—and to mitigate exposure and potential liability. Counsel should also be used to engage all other vendors to protect privilege.

Involve your broker and cyber insurer right away. Your broker can help give timely notice to the appropriate insurers and advocate for coverage. Your cyber insurer will need to be involved from the outset in order to consent to all costs before they happen.

To avoid conflicts with your cyber insurer, know whether your policy allows choice of counsel/vendors or requires the use of panel firms. Most cyber insurers have lists of pre-approved vendors that include breach/privacy counsel, forensic experts, notification and call center providers, and public relations firms. Decide which firms you intend to engage before a cyber event happens so you aren't stuck making those decisions in the middle of the crisis.

5.0 CONCLUDING PERSPECTIVE

Return to Table of Contents >>

A MESSAGE FROM

Carolyn Polikoff

National Commercial Lines Practice Leader

REACH OUT TO CAROLYN >

With cyber liability insurance becoming more ubiquitous, more unpredictable, and, in some cases, more confusing than ever, it's critical to have a comprehensive guide to the trends we're noticing in the cyber market and what you should know going into 2022.

Like most insurance markets this year, the cyber market is reeling from the past two years' volatility. As described in this first-ever *Guide* focused on cyber risk, we're watching issues like the increases in ransomware attacks and the costs associated with these events (which are driving sharp reactions from underwriters), supply chain attacks that highlight the problem of aggregated risk, plus concerns like: privacy regulations, mass arbitration, and how to respond to a breach. All told, there is much for the modern business to be cognizant of.

Based on the results of our Underwriters' Survey, most insurers expect increasing cyber risk as well as increasing cyber premiums going into 2022. Now more than ever, it's clear that having a knowledgeable, trusted cyber insurance broker in your corner is key to navigating the current complex market.

We're pleased to share this first cyber liability-focused *Guide* that is a complement to Woodruff Sawyer's annual *Looking Ahead Guides* for **D&O Insurance** and **Property & Casualty**. Wherever the next year takes us, Woodruff Sawyer will be there to champion for our clients' needs with expert advice and fierce advocacy.

Additional Resources

The Cyber Notebook >

Woodruff Sawyer Events >

The D&O Notebook >

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

Woodruff Sawyer Insights >

Return to Table of Contents >>

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 & 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. If you have any questions or comments regarding the Looking Ahead Guide, please contact your Woodruff Sawyer Account Executive or email us at: **LookingAhead@woodruffsawyer.com**.

For more information

Call 844.972.6326, or visit **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 related to Business Risks and/or Employee Benefits.

WOODRUFF SAWYER

WOODRUFF-SAWYER & CO.

AN ASSUREX GLOBAL & IBN PARTNER

woodruffsawyer.com