RISK strategies

2023 Cyber Liability

Building cyber resilience in a complex world

Table of Contents

Introduction

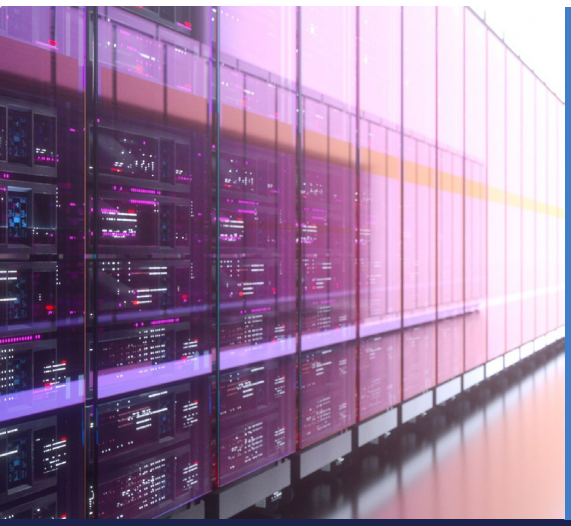
It is hard to model cybersecurity risk. Unlike health insurance where underwriters can look at claims experience, medical care inflation, and demographics to estimate future costs, historical cyber data can't predict what cyber criminals will cook up next.

However insurers are using data to understand systemic risks and inform best practices to manage cybersecurity risk. Every breach and forensics examination reveals vulnerabilities and mitigation strategies. Acting on this knowledge is key to protecting your organization, maximizing the cyber coverage you qualify for, and minimizing rate hikes.

The challenge? It is difficult to stay current on the threat landscape and one step ahead of bad actors. Adhering to cyber best practices has become a condition for buying and retaining coverage, and insurers are requesting proof of your defensive strategy.

By now, most organizations have implemented mandatory annual cyber awareness training for all employees, covering topics such as phishing and social engineering attacks. While this education is thwarting cybercrime, it is only part of a robust defense strategy. So, what is next?

This eBook looks back at the state of cyber in 2022, highlights important developments, and describes what to expect in 2023.



Today, virtually every organization relies on data, so no one is immune from cyber threats. We appreciate the opportunity to partner with you to protect your digital assets with the right insurance coverages.

State of the Cyber Liability Market

Market Updates

The cyber insurance market has started to stabilize after years of steep rate increases, but insurers will continue to be on high alert in 2023 and beyond.

Ransomware claim activity persists, and business email compromise and funds transfer schemes remain an ongoing issue. Insurers are also concerned about the potential for a systemic event where a threat actor infiltrates a cloud or other service provider, which then compromises customers' security.

However, the pace of attacks slowed in 2022 due to several factors including better awareness and cyber maturity in the marketplace, driven by increased underwriting scrutiny over the last 24 months.

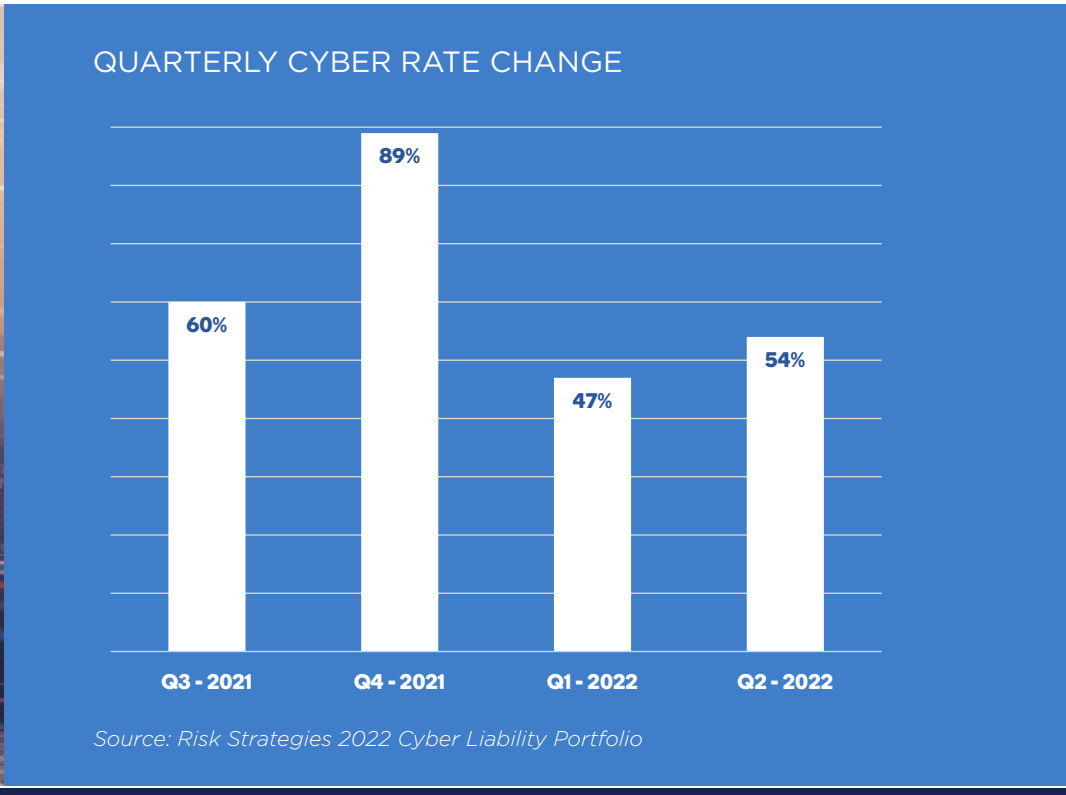
Carriers are still being conservative and restrictive on coverage, limiting their exposure to ransomware claims and systemic events in certain instances where controls still require improvement.

Coverage Considerations

The first two quarters of 2022 saw 50% rate increases on average, but Q3 decelerated to increases in the 30% - 40% range. Buyers with claims and industries with historically adverse claims experience are still seeing increases well in excess of market averages. Insurers are focused on proper risk selection, and buyers failing to prioritize proper cyber controls are struggling to maintain and secure the full breadth of coverage or in some cases any coverage.

In a market absent of a catastrophic event, there should be further stability in 2023. As evidenced by the Risk Strategies rate index, we have seen rate deceleration amongst our client base in the last two quarters. Excess rates are beginning to come down due to new capacity entering the market, which is usually a precursor to further softening of primary layers.

Risk Strategies believes rate increases could get down to the 10% - 25% range in 2023 under the right conditions.



Source: Risk Strategies 2022 Cyber Liability Portfolio

Threats and Optimism Grow in the Volatile Cyber Market

Cyber insurance has undergone continuous change over the past decade and evolved into one of the most complex and important coverages an organization can have in their toolbox. The cyber insurance market is challenging and volatile. However, with enterprise-wide adoption of proper protocols, an organization can weather the storm.

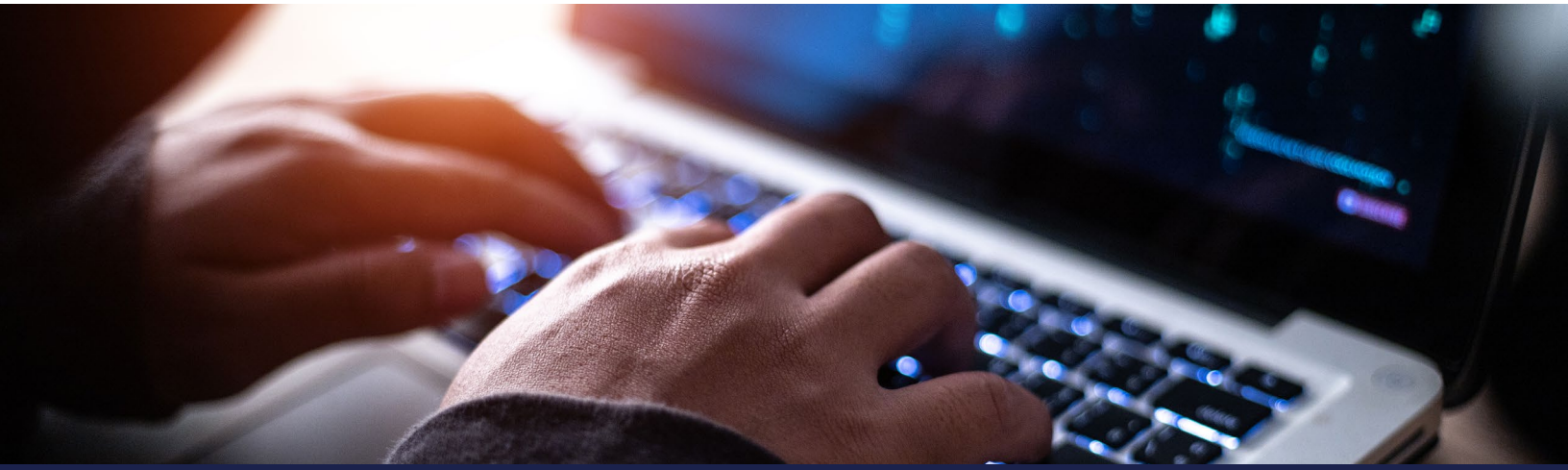
Policy Evolution

Initial protection for cyber-related risks was covered by "silent" cyber coverage buried in other insurance policies such as property, general liability, professional liability, and/or kidnap & ransom.

As businesses' reliance on technology grew, insurance carriers gained awareness of cyber-specific risk and silent cyber coverage was replaced by standalone cyber policies.

When standalone cyber insurance was first introduced, insurers largely saw the revenue potential and focused on gaining market share. This created a competitive environment with overly broad policies and competitive pricing. What insurers may not have fully appreciated, or priced in, was how large and expensive cyber losses could be — especially in light of the evolution of cryptocurrency and ransomware claims.

In recent years, as threats and incidents escalated, so did cyber claims — in the form of more frequent and larger loss payments. Threat actors have been relentless as gains from their endeavors have increased. Insurers are taking corrective action on their portfolios by increasing premium rates, adding restrictive language, and carefully underwriting risks.



Growing Threats and Issues

The following issues are driving industry-wide change:

- **Mounting Claims:**

  Due to increased frequency and severity of ransomware attacks, cyber claims have rapidly grown in scope and expense.

- **Regulatory Action:**

  The regulatory environment and enforcement of associated fines/penalties continues to evolve, notably at the state level.

- **Expanding Attack Surface:**

  The proliferation of endpoint devices has created additional points of entry for threat actors.

- **Systemic Risk Potential:**

  Many businesses rely on third-party vendors for essential services. If a threat actor were to target a major cloud provider, the resulting impact could compromise thousands of businesses simultaneously.

Looking Ahead: A Reason for Optimism

Despite hardening market conditions, there is reason to believe that rates may soon start to plateau for insureds who meet the carriers' standards and display ongoing cybersecurity efforts. Compared to 24 months ago, organizations are better educated about potential threats and have implemented controls to mitigate cyber risks. However, for businesses that do not meet the minimum standards or make the necessary investments, cyber insurance may no longer be a feasible option.

The future of risk in the cyber landscape will require businesses to institute best practices, which will continue to change, and to continually educate themselves and their employees.

Cyber Insurance for Public Companies Under New SEC Proposal

On March 9, 2022, the SEC voted to propose significant new rules that would enhance and standardize public company disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting.

If adopted, the rules will put additional compliance burdens and reporting obligations on public companies that they will need to be prepared for. Cyber insurance will grow in importance, as investors will view cybersecurity as a material risk. Our practice is analyzing these impacts so we can provide you with the necessary insights and advice.

In adopting the proposal, the SEC cited the growing threat of serious cybersecurity attacks and the utility of consistent and comparable cybersecurity information for investors to more efficiently allocate capital. The new rules would apply to all public companies subject to the reporting requirements of the Securities Exchange Act of 1934.

The proposal would impose two new types of disclosure requirements: (1) disclosure of cybersecurity incidents and (2) disclosure of cybersecurity risk management, strategy, and governance.

The public comment period ended in May 2022, but as of the end of 2022, there was still no timeline for legislative approval and implementation.

Most notably, the proposal requires companies to disclose information about a "material cybersecurity incident" within four business days of determining that the incident is material. The proposal defines "material" by the standard applicable to other securities laws: namely, whether "there is a substantial likelihood that a reasonable shareholder would consider it important." The proposal includes specific information companies would be required to disclose about any material cybersecurity incident.

"

Most notably, the proposal requires companies to disclose information about a "material cybersecurity incident" within four business days of determining that the incident is material.

In addition, the proposal would also require companies to provide any material changes or updates to previously disclosed cybersecurity incidents. Disclosure would be required "when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate."

Apart from the cybersecurity incident reporting, the proposal would require "enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance." As to risk management and strategy, it would require companies to adequately describe the procedures they have in place, if any, for the "identification and management of risks from cybersecurity threats."

Companies would also have to describe their board's "oversight of cybersecurity risk," including identifying which board members or committees oversee cybersecurity risks and the frequency with which the board discusses cybersecurity risks.

Outside of the boardroom, the proposal would also require disclosure of how the company's management assesses cybersecurity-related risks, including a description of the persons or committees managing cybersecurity risk and a description of the expertise of any chief information security officer. Under this proposal, public companies will need to specify the cybersecurity expertise of members of the board of directors, if any.

In a 2022 public address, SEC Chair Gary Gensler outlined six areas where he had asked SEC staff to consider cybersecurity-related regulations. With the announcements of proposed SEC rules affecting public companies and previously-announced rules for investment advisers, there remains a strong possibility of further cybersecurity proposals addressing broker-dealers, Regulation SCI, Regulation S-P, and third-party financial service providers.

In other words, there is almost certainly much more to come. As a result, it is imperative for companies to review their cyber insurance strategies sooner rather than later to be prepared for the potential impacts of these sweeping new regulations in the field.

Systemic Risk Assessment for Increased Cyber Protection

With the ever-growing threat of bad cyber actors disrupting critical processes, a systemic risk assessment of potential cyber vulnerabilities is more important than ever. From an insurer's perspective, the benefits of establishing best practices for doing so extend to every activity, from businesses large or small to Private Client concerns.

On its face, this assessment can be a daunting task. Whereas most cyber events have a narrowly defined set of victims, a systemic cyber incident could do damage on a national or even a global scale — threatening the digital infrastructure that entire societies, economies, and governments rely on to function.

The growth and scope of these threats ripple through the cyber insurance industry. Underwriting requirements have tightened, and for many insureds, CBI (Contingent Business Interruption) policies have been sub-limited as a cost-containment strategy — for instance, a client may carry a $10 million policy limit, but CBI is sub-limited to only a small portion, i.e., $250,000. This is generally far less than will cover actual losses an insured may suffer in the event of a devastating cyber attack.

What are the key steps insureds can take to not only safeguard themselves against cyber attacks, but also satisfy systemic risk underwriting requirements for more thorough protection within their cyber insurance coverage? Here are a few important recommendations:

Develop Strong Vendor Relationships and Controls

Contracting with established, reputable vendors is the first and most obvious step to take to protect infrastructure and demonstrate the robustness of internal controls to underwriters.

From a broader perspective, as businesses increase their reliance on outsourcing for information technology products and services, vendor risk management (VRM) has become a crucial component of any enterprise risk management framework. It is in the best interest of your organization to manage vendor risks before, during, and after a vendor relationship ends. VRM ensures that third-party products, IT vendors, and service providers do not lead to business disruption or financial and reputational damage.

Stay on Top of Critical Patching

Implementing well-structured patch management is a part of the process for organizations to become cybersecurity compliant. Recent studies indicate that poor patch management accounts for as much as 57% of data breaches. A poor patch management system leaves sensitive data exposed and easily susceptible to malware and ransomware attacks.

Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment). Timely patch management helps maintain operational efficacy by correcting software errors detected after release, and by mitigating security vulnerabilities.

Although many organizations handle patch management on their own, some managed service providers perform patch management in conjunction with the other network management services they provide. If your organization goes this route, consider the vendor relationship risks involved.

Implement a Strong Risk Management Framework

For firms of any size or classification, establishing a risk management culture and the infrastructure to support it is essential. Implementing a successful risk management program means detailing how a firm identifies, analyzes, evaluates, treats, and manages risk.

A well-designed, all-inclusive risk management framework provides a roadmap to avert corporate disaster and competitive disadvantages, and demonstrates the types of controls that underwriters look for in determining a firm's insurability. A well-developed program will detail controls in multiple areas, including:

- Marketing and communications
- Recruiting and human resources
- Information and resource management
- Product development
- Regulatory obligations
- IT issues and security
- Succession planning
- Acceptance and continuance of clients
- Cash flow management

Create Thorough Business Continuity & Disaster Recovery Plans

As we have seen too often over the past few years, major cyber attacks happen even to the best-prepared organizations. When breaches do occur, firms need to have detailed and nimble business continuity and disaster recovery (BCDR) plans in place.

The term "cyber resilience" refers to a business's ability to continuously deliver on its intended outcome despite adverse cyber events. Implementing a cyber resilience strategy as

> A systemic cyber incident could do damage on a national or even a global scale — threatening the digital infrastructure that entire societies, economies, and governments rely on to function.

part of your company's BCDR plan can ensure that the organization can continue operations, perhaps at reduced capacity, even in the face of ongoing attacks.

Engage with Specialty Brokers

The cyber risk landscape is continually shifting, and new threats continue to emerge. By acting robustly to protect your interests, you also provide an added layer of security for interconnected businesses and drivers within the global economy.

A key component of systemic risk assessment is engaging with a cyber insurance specialty broker, especially one that can serve both business and private client needs. We can help to identify the latest trends, emerging areas of concern, and recommended best practices to assure that your cyber coverage provides optimal protection for your business.

What to Expect in 2023

Rather than manage cyber insurance costs by estimating the financial risk, insurers are limiting exposures through restrictive underwriting and strategically managing capacity in the case of a systemic cyber event. Your organization's cyber maturity is a primary factor in determining insurability, coverage amounts, and pricing.

A cyber-aware workforce and multi-factor authentication have become table stakes. Without these safeguards, your likelihood of getting a cyber policy is negligible. In 2023, we anticipate insurers will request additional defensive measures and documentation.

Five Tips for 2023

1. Expand your endpoint security planning

Hackers will find clever new ways to infiltrate your network through endpoint devices. With edge computing and the proliferation of smart devices that connect to company resources, endpoint security has become exponentially more complex. Medical devices, fire alarms, and other equipment not typically owned by IT now require cybersecurity protocols.

2. Examine the software/platform/infrastructure as-a-service products you rely on

Though SaaS, PaaS, IaaS, and other as-a-service offerings provide convenience and cost-savings, they complicate your security planning and increase systemic risk potential. Have you established a service-level agreement with each provider regarding cybersecurity? No matter what security promises you receive from a vendor, your organization bears ultimate responsibility for protecting data and meeting customer needs. If a breach occurs in a vendor's network, your customers expect you to have a Plan B.

3. Pause training at your own peril

Employers who are belt-tightening due to the economy often view training as discretionary spending, as opposed to a necessary investment. But people are your first line of defense against cyber threats, and insurers expect your workforce to practice good security hygiene and to know what danger signals to watch for.

Additionally, those involved in software development, IT ops, data pipeline management, and other specialty roles need in-depth knowledge of how to spot and correct vulnerabilities. For example, many software development teams are shipping code today with security vulnerabilities. Does your organization include security protocols when defining software requirements? Have you implemented secure coding best practices and trained your teams on these? Are you monitoring compliance to make sure all developers are adhering to the coding standards you've established?

4. Look at corporate culture and compensation through a cyber lens

Some executives reward product development speed in a way that compromises cybersecurity. If their bonus depends on getting a new feature to market by a specific date, what prevents them from taking security shortcuts?

If you measure software developers' performance based on the number of tickets or story points, do they have incentive to focus on cybersecurity?

You need to audit your business to identify practices that may be creating inadvertent cyber risk.

5. Consider the impact of layoffs on cybersecurity

A reduction in force — within your company or at a vendor you use — can open the door to multiple cybersecurity risks. People with institutional knowledge of vulnerabilities can use that information to harm an employer. Handling a layoff poorly with inadequate notice and impersonal communication can leave you (or a vendor) with a disgruntled workforce. One upset employee can bring your system down.

The surviving workforce, which is now shouldering a heavier workload, may be tired. Fatigue can lead to human error and oversights, such as failing to monitor open ports or clicking on a malicious link.

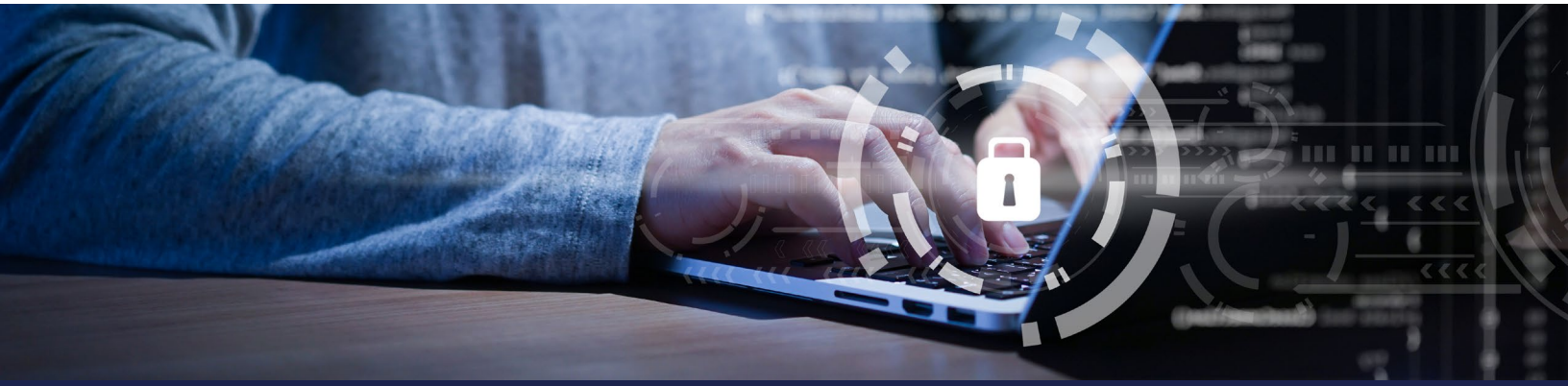
If heavy layoffs take place in a compressed timeframe, certain job tasks may sit completely neglected, including those related to security monitoring.

Hackers watch for signs of internal turmoil and pounce on your vulnerabilities. If you are busy quelling a media firestorm, are you paying adequate attention to your cyber defenses?

From a compliance mindset to a security culture

As authorities crack down on one type of cybercrime, bad actors find new ways to infiltrate your network. Because the human imagination is limitless, the cyber threat landscape will continue to expand and morph.

Instead of viewing security as a checkbox and implementing bare minimum defensive activities, you will need to do more in 2023 to qualify for the best cyber insurance rates and provisions. Together, we can talk through what a security culture looks like and how to get from where you are today to a state of cyber resilience.



Risk Strategies Cyber Practice

Facing increasing cyber threats, stringent regulations, and potentially significant financial and reputational harm, Risk Strategies Cyber Liability insurance specialists deliver comprehensive products and services to keep you safe including:

- **Assessment and Analytics —** For key vulnerabilities, threats, claims trends, loss modeling, and limit benchmarking
- **Risk Mitigation —** Providing action plans for areas of improvement with tabletop exercises, employee training, and incident response planning
- **Comprehensive Cyber Coverage —** Specialty market knowledge, broad real-world experience, and strong relationships with key insurers at the best available price
- **Cyber Resolute —** A proprietary, market-leading coverage solution for clients under $250M in revenue, underwritten by Berkley Cyber Risk Solutions
- **Dedicated Cyber Risk Response and Claims Advocacy —** Including specialty claims advocates and in-house counsel to deal with coverage issues and ensure maximum recovery under your policy
- **24/7 Monitored Email and Phone Hotline —** So you can contact our team about data security incidents at any time of the day or night

Today we serve more than 2,000 cyber clients across diverse industries.

Industry Experts

Rob Rosenzweig
National Cyber Risk Practice Leader

Allen Blount
Cyber Team Leader

Kathleen Curley
National Account Director

A Trusted Partner

Risk Strategies is the 9th largest privately held US brokerage firm offering comprehensive risk management advice, insurance and reinsurance placement for property & casualty, employee benefits, private client services, as well as consulting services and financial & wealth solutions. With more than 30 specialty practices, Risk Strategies serves commercial companies, nonprofits, public entities, and individuals, and has access to all major insurance markets. Risk Strategies has over 100 offices including Boston, New York City, Chicago, Toronto, Montreal, Grand Cayman, Miami, Atlanta, Dallas, Nashville, Washington DC, Los Angeles, and San Francisco.

STAY INFORMED, STAY ALERT, AND STAY TUNED.

Connect today with the Risk Strategies Cyber Liability insurance team to get a specialist approach to your risk.