



CYBER INSURANCE:

THE UNSUNG
INVESTMENT
HERO

Part 4:

*Not All Brokers Are Created Equal:
Importance of Investing in the Best Partner for
Placing Cyber Insurance*

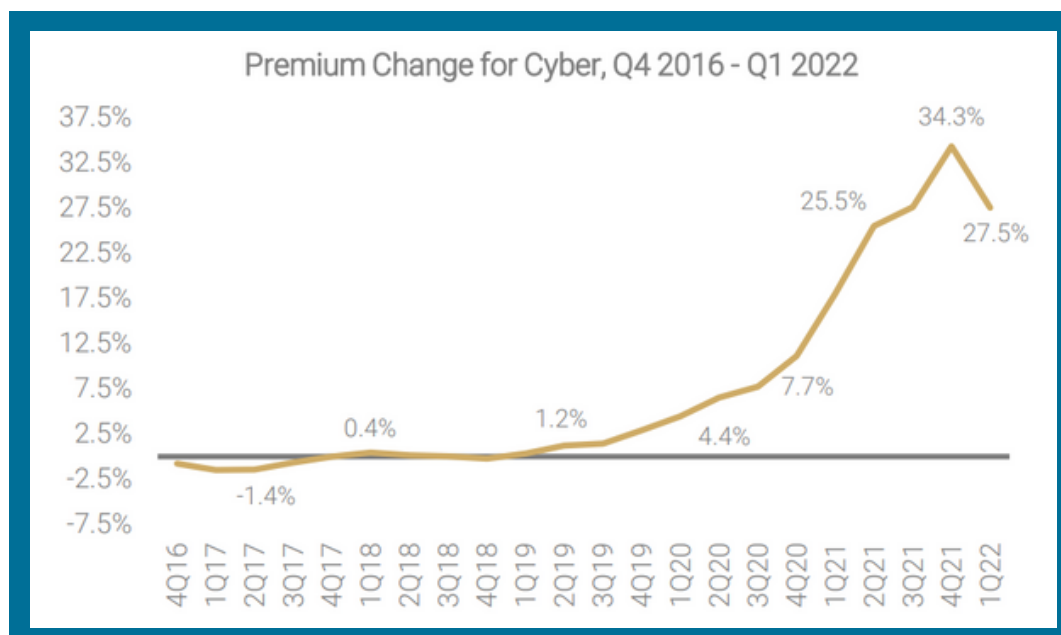


THE
**CAPITAL
GROUP**
A BALDWIN RISK PARTNER

Not All Brokers Are Created Equal: *Importance of Investing in the Best Partner for Your Cyber Insurance Needs*

YOU MAKE A LOT OF INVESTMENTS IN YOUR BUSINESS.
BUT CYBER COVERAGE COULD BE ONE OF THE MOST IMPORTANT.

From knowing your cyber risk and [how to quantify it](#), understanding the [return on investment](#) on cyber insurance, and [deciphering the policy language](#), it is clear that navigating the cyber insurance marketplace is a complex undertaking. Additionally, a surge of losses and economic strains brought on by the COVID-19 pandemic, increasingly sophisticated attack patterns, and heightened demand for coverage have caused the cyber insurance market to harden, making finding and placing cyber coverage increasingly challenging with each passing year.



According to a report from the **Council of Insurance Agents and Brokers** there was a:

25% increase in prices for cyber coverage for 5th consecutive quarter

26.8% average premium increase

Though carriers continue to tighten underwriting standards and provide less favorable terms for coverage at a higher cost as a response to diminished capacity and unprecedented losses, the reality is that businesses need to meet the standards set forth by carriers in order to get cyber coverage. Cyber coverage is crucial for any organization that seeks to protect its reputation, finances, and operations in the event of a cyber incident.

Investing in the right broker with proven experience placing coverage and connections in the cyber marketplace is a value add to your risk management strategy.

Here are some ways partnering with a knowledgeable broker will help you maximize your investment in cyber insurance:



1 RISK AWARENESS AND STRUCTURING COVERAGE

Getting the right cyber coverage is not like shopping for car insurance. Cyber policies have evolved to the extent that you have to consider dozens of endorsements, coverage parts, exclusions, limits, sublimits, premiums, and deductibles... the list goes on. Understanding policy terms is difficult for the average consumer. On top of this, most companies do not know what their cyber risk looks like, and without having an understanding of cyber exposure, you cannot determine how to structure cyber coverage for your unique risk profile.

A seasoned broker will take the time to discover which parts of your business are connected to technology, how that may create risk for your business, and become deeply familiar with your operations, its people, and your culture. They should also possess robust knowledge about the capabilities and limitations of cybersecurity controls when it comes to protecting your company, and in terms of the human capital that it will take to implement and maintain them. By taking this approach, a broker can then provide recommendations for coverage so that you are neither over nor under insured.

2 NAVIGATE CHANGES FROM CARRIERS

Because the cyber landscape changes rapidly and frequently, carriers often change their requirements for coverage to try and keep pace with evolving risks. For many years, cyber insurance was underpriced relative to the amount of vast cyber exposure that exists. When the number of cyber claims increased exponentially in the wake of the COVID-19 pandemic, carriers became overwhelmed with losses. They decided to look back at their profit and loss statements, how these losses occurred, and what could have prevented them. Based on these findings, they began to require multi-factor authentication (MFA) from insureds to even consider providing coverage.

Though most organizations now know that they need MFA, cyber carriers continue to add on to the list of required cybersecurity tools and practices that insureds need as they learn more about things that can be done to prevent the likelihood of a cyber incident. More carriers now require evidence of best practices for remote desk protocol, encrypted backups, implementation of endpoint detection and response solutions, use of a virtual private network, and an incident response plan. These changes from carriers come quickly and without warning. For the most part, you have to adhere to them if you want coverage.

An effective broker has strong relationships with carriers, which gives them access to this crucial information as it comes out. If there are changes to requirements for coverage, your broker should communicate with you as soon as possible, even if it is not time for your renewal. A good broker will then help you develop a strategy going into renewal that demonstrates that you are able to adhere to the new requirements so the carrier does not decline your coverage.

3 BREAK DOWN COMMUNICATION SILOS

Underwriters are much more hesitant to take on risks they cannot predict or fully understand. If you are unable to provide them with a full and accurate picture of your cybersecurity posture, then you will likely get declined. An experienced broker will take a deep dive into understanding your business inside and out, help the underwriters fully understand it and the risks you face, and communicate the loss controls you've implemented to proactively help prevent claims from a cybersecurity incident. Being able to paint this picture is contingent on breaking down communication silos within your company and with carriers.

After familiarizing themselves with your business, an experienced broker will engage your IT team and any insurance purchasing decision makers so that all relevant parties understand the importance of investing in cybersecurity and their respective roles and responsibilities in applying best cybersecurity practices.

The right broker will also create an open channel of communication between your business and the carrier. After building a cohesive strategy with your company's internal stakeholders, your broker should coordinate a call that includes themselves, your insurance decision makers, your IT team, the underwriter, and the carrier's cybersecurity experts.

By the end of the call, you should understand the following:

- The underwriter's requirements going into the renewal for them to offer coverage
- If the carrier can offer the same previously held limits
- The reasons for rate increases
- How to access resources if you need assistance implementing cybersecurity loss controls and cybersecurity protocols
- Next steps needed to get coverage

4 NEGOTIATE POLICY TERMS

If a carrier gives you a quote that you feel is too high or declines your business for coverage, **an experienced broker will uncover the reasons behind the denial and negotiate on your behalf.** In instances when you might not have the cybersecurity practices or tools in place that a carrier requires, your broker might be able to reach an agreement with the carrier where you are able to get coverage that is contingent upon you meeting the standards for coverage by a certain deadline.

Another common scenario that might require your broker's advocacy is if your business has had a cyber claim in the past. If this is the case, the right broker will know how to communicate effectively both with you and the carrier to build a detailed narrative that shows how the loss happened and the corrective measures you took or are taking to prevent it from happening again.

In less than ideal scenarios, the best brokers will advise you about what you should do to better position your business for coverage and leverage their existing relationships with carriers to negotiate on your behalf to obtain better market results.

5 ACCESS TO MARKETS

In worst case scenarios, carriers might still decline coverage with no room for negotiation because there are certain protocols, underwriting guidelines, and/or rules that are totally inflexible. Should this be the case, the best brokers are of the mentality that they will do whatever it takes to at least get you one quote and deploy all the resources and tactics we've delineated above (negotiating and crafting a risk management narrative). Top-tier brokers will have market access for difficult risk profiles even in a hardened cyber insurance landscape. A broker needs to have great relationships with reputable carriers to get things done.

In worst case scenarios, carriers might still decline coverage with no room for negotiation because there are certain protocols, underwriting guidelines, and/or rules that are totally inflexible.

6 PROVIDE ACCESS TO RESOURCES

You might need guidance about implementing best cybersecurity practices at your organization and determining which tools you should purchase to improve your cybersecurity posture. Or maybe you have limited resources you can allocate to achieve your cybersecurity goals.

In this situation, your broker should have access to legitimate resources and information that they can pass along to you, so you have the right cybersecurity tools in place and develop a culture of cybersecurity within your company.



CONSIDER ASKING THE FOLLOWING QUESTIONS IF YOU ARE CURRENTLY LOOKING FOR A BROKER TO HELP YOU FIND CYBER COVERAGE:



- ☐ How do you familiarize yourself with a company's unique risk profile?
- ☐ What does your process look like for properly structuring cyber coverage for your clients?
- ☐ Do you have experience working with similar clients?
- ☐ What will you do to help me understand the ins and outs of my coverage?
- ☐ How have you advocated for clients in the past when they were met with unfavorable terms for coverage or were declined?
- ☐ How do you stay abreast of cybersecurity trends and carrier requirements?
- ☐ Do you have a team that specializes in cyber insurance coverage?
- ☐ Can you speak to your relationships in the cyber insurance market?
- ☐ Which cybersecurity resources can you connect me to?
- ☐ What is the process for managing cyber claims?
- ☐ Do you have references you can provide?

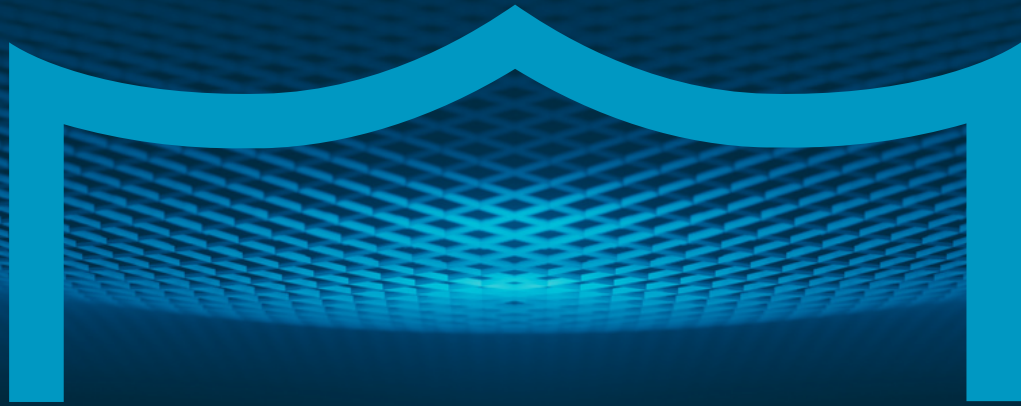
If your existing or prospective broker cannot provide satisfactory answers to these questions, then they might not be the right broker for your needs. By investing in the right broker, you gain the peace of mind of knowing that your best interests are accurately represented in front of carriers, and that you can adapt to the everchanging cyber risk landscape. Our team is committed to these values. We strive to become an extension of your team and deliver cyber risk mitigation strategies and insurance architecture that align with your overarching risk containment strategy.



Contact us to learn more about how investing in the right broker partnership renders the best possible results for your unique cyber exposures.

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.





CYBER INSURANCE:

THE UNSUNG
INVESTMENT
HERO



THE
CAPITAL
GROUP
A BALDWIN RISK PARTNER