# CYBER INSURANCE:

## THE UNSUNG INVESTMENT HERO

## Part 1:

*Quantifying Cyber Risk &*
*Proving the Value of a Cyber Insurance Investment*

AHT INSURANCE
A BALDWIN RISK PARTNER

# WHEN IS THE LAST TIME YOU QUANTIFIED YOUR CYBER RISK?

## *Creating a Cyber Risk Balance Sheet & Proving the Value of Cyber Insurance*

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

The headlines are everywhere. It seems like every day there is news about the target of a cyber breach or the increasing severity and sophistication of cyberattacks. People and organizations continue to rely more and more on digital connectivity—a reality that is unlikely to change. The opportunities brought on by technology will continue to come with cyber risk, which is why businesses of all sizes and industries need to invest in cybersecurity and cyber insurance in their overarching approach to risk management.

Digital risk is dynamic, and this makes it challenging for businesses to understand the scope of their cyber risk. If organizations do not know how to quantify this risk, they might find it difficult to justify or know how much to invest in their cybersecurity posture and cyber risk management. **Cyber risk quantification practices, including cyber risk modeling, evaluating the amount and type of confidential information held, determining the location of those digital assets, and creating a hierarchy of those assets are a good start.**

Quantifying your cyber risk by creating a cyber risk balance sheet empowers you to properly structure and invest intelligently in cyber coverage so that it's best aligned with your company's risk mitigation strategy.

AHT INSURANCE
A BALDWIN RISK PARTNER

# CREATING A CYBER RISK BALANCE SHEET

Developing a cyber risk balance sheet is something that improves decision-making around cyber risk management by aligning cyber security within the context of your overall risk management strategy. You will need to closely align yourself with your cybersecurity IT leaders, as they will need to document cyber events that can impact your company's finances.

**Here are the key steps involved:**

1. **Quantification framework:** You need to have a framework to quantify risk that aligns with your company's risk profile. Industry-accepted frameworks like FAIR and NIST provide a reliable basis from which you can estimate the direct and indirect costs associated with cyber risk. However, since there is no standardized way to quantify cyber risk, cyber leaders might find it challenging to determine how they can properly measure it. Tools like CyberCube, available to BRP clients, use insurance data and proprietary modeling to help with this framework.

2. **Cyber threat identification:** After determining a quantification framework, your cybersecurity team will need to identify cyber threats, the probability of the cyberattack happening, and vulnerable critical assets. They also need to identify cyber controls and practices that are in place and their effectiveness in protecting your company.

3. **Correlation of threats to finances:** Having detailed data about current and emerging threats allows cyber leaders to correlate how different impact scenarios (from smaller to extreme losses) affect your company's finances. Your cybersecurity team needs to be able to translate complex, technical jargon into consumable and actionable insights. This enables other stakeholders to fully grasp the financial, operational, and reputational impacts of a company's cyber risk and make informed decisions about their investment in cybersecurity and cyber insurance.

## IMPLEMENTING A CYBER RISK BALANCE SHEET

After developing a cyber risk balance sheet, it's important for all relevant business units to continually engage with one another. Your company's cyber leaders and financial decisionmakers should periodically review and iterate your cyber risk balance sheet. This ensures that investments in cyber security and risk management are rendering the desired ROI, and that cyber risk mitigation investments adapt and meet your business' evolving risk profile.

Do not be afraid to ask questions that challenge calculations, as this helps ensure more accurate estimations about what your cyber risk amounts to. Hold teams accountable to outcomes. This reduces the possibility of a cyberattack severely impacting your bottom line. Breaking down communication silos between business units is key to optimizing your investment in cybersecurity.

**In the context of insurance, taking collaborative, proactive steps to understand your cyber risk shows carriers that your organization has a culture of cybersecurity, which usually amounts to more favorable coverage terms.**

## INSURANCE AND RISK TRANSFER STRATEGIES

Though you can work toward continually implementing the best tools and practices to protect your business from cyberattacks, there is no airtight solution that can prevent them completely. Unfortunately, breaches can occur even with the most stringent cybersecurity measures in place. According to the NetDiligence 2021 Claims Study, staff error and phishing emails are two of the top five triggers of claims. Bearing this reality in mind, your cyber risk balance sheet needs to include strategies and investments you can make to protect your business from cybercrime.

**Cyber insurance is one of the best ways to protect your business. Purchasing the right coverage can help you transfer some of your cyber risk to an insurance company.** Deploying a data backed risk quantification strategy will give you an idea of what your actual risk amounts to in financial terms. These insights should inform how you choose to structure your cyber coverage in terms of limits, premiums, and deductibles, in addition to any endorsements, coverage parts, and exclusions that can impact the type of coverage you need for your business.

**A well-structured cyber insurance policy does many things beyond provide coverage, and this includes incident response assistance after a breach.** Many carriers also offer risk management tools and services – making cyber insurance is an important part of any organization's overall risk management strategy.

You also need to look at how contracting with other parties can create cyber risk for your business. Most companies rely on third-party service providers and vendors to support their business, introducing new layers of risk to data security and operations. Vendors oftentimes need access to internal systems and sensitive data, which creates additional risk. When you are entering an agreement with vendors and service providers, all involved parties need to think about how cyber risk fits into the picture. These are some steps you can take to effectively manage that risk:

**These are some steps you can take to effectively manage that risk:**

- **Vet all vendors:** Prior to engaging with a vendor that will have access to your network or any sensitive data, you need to review their approach to cyber security. Do they have an incident response plan? Do they regularly train employees about cyber security? What cybersecurity policies do they have in place? Are there limits to their indemnification in the event of an incident? Do they also carry comprehensive Cyber and Technology E&O policies?

- **Implement & Understand Contracts:** One of the most important things to take into account when assessing your cyber risk is the contractual relationships you have with vendors and clients. You need to have a contract in place for the exchange of services that clearly addresses the vendor's obligations and rights pertaining to confidential, personal data and any cyber insurance requirements. If possible, the contract should place certain obligations on a vendor if a breach or technology failure were to happen.

# CYBER RISK AND CASH FLOW MANAGEMENT

Organizations need to understand how their cybersecurity posture correlates to business consequences and be prepared to rebound in the event of a cyberattack. A successful attack can cause devastating financial disruption for your business or even shut it down, which is why they are one of the top risks for financial stability. Creating your cyber risk balance sheet and contextualizing it within your cash flow management strategy can help you better mitigate risk in an unpredictable economic environment. If an outage caused by a cyber incident shuts down your network and operations – how much time will it take to restore? What does that mean in terms of lost revenues?

## HOW CAN YOUR BROKER HELP?

Quantifying your cyber risk and knowing which tools and risk mitigation strategies are worth investing in is challenging. An experienced broker can help you determine what your risk is, provide resources to help you improve your cybersecurity posture, and find cyber insurance that meets your unique risk profile. Our team has seen countless scenarios play out and has the experience to learn the ins and outs of your business and discover how parts of your business connect with technology to create risk. This allows us to provide recommendations about how you can best invest in cyber insurance to protect your business from the unexpected. Cyber risk modeling is available to help answer some of these questions surrounding quantification. BRP has special access to these resources to help answer some of the questions posed above.

**Contact us to learn more about how we help manage your cyber risk.**

# CYBER INSURANCE:

## THE UNSUNG INVESTMENT HERO

## Part 2:

*Understand the ROI of investing in Cyber Insurance*

AHT INSURANCE
A BALDWIN RISK PARTNER

# IS IT WORTH IT?
# Understanding the ROI of Cyber Insurance

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

With organizations facing more cyber threats than ever, one of the greatest challenges for business leaders is understanding the return on investment (ROI) of cybersecurity initiatives. Economic pressures have negatively impacted operational costs in recent years, so it only makes sense that you want to know that the investments you make in your business are rendering positive results.

There is a direct correlation between the evolution of cyber risk and the resources you invest in your cyber risk mitigation. **Taking the time to calculate the ROI of cybersecurity initiatives only empowers you to understand the financial impact a breach can have on your organization, which better positions you to rebound in the event of a cyber incident.**

When cybersecurity and business leaders work together to quantify cyber risk and determine the financial implications of a breach, this helps create a culture of cybersecurity that ultimately benefits your overarching risk strategy and protects your balance sheet. Time and time again, cyber insurance proves itself to be one of the most valuable investments you can make to financially protect your business from the consequences of a cyber event.

AHT INSURANCE
A BALDWIN RISK PARTNER

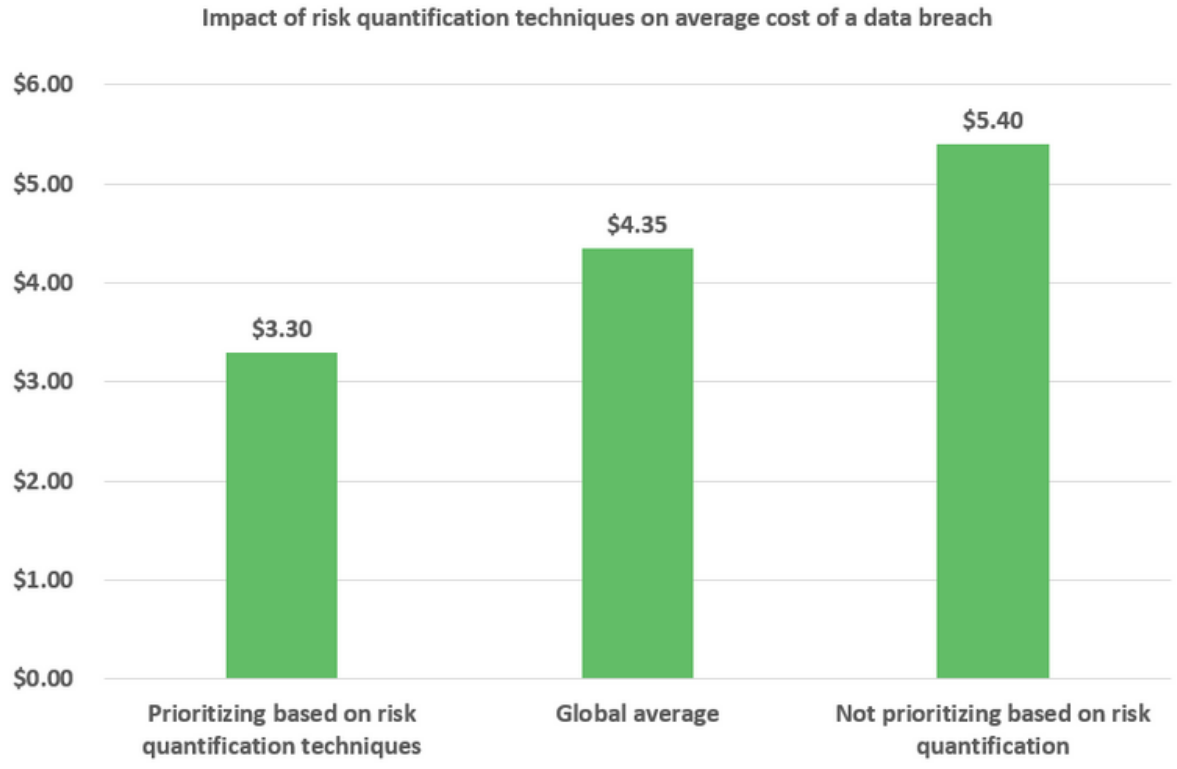
# CHALLENGES: DEMONSTRATING THE VALUE OF CYBER RISK MITIGATION INVESTMENTS

The reality is that calculating cybersecurity ROI is notoriously challenging because there are many factors that come into play. Beyond the potential loss of dollars and cents, it is also important to consider potential losses from stolen intellectual property, business disruption, and damaged reputation. Reliable resources can be hard to come by due to the lack of sustained loss data and the constant and rapid evolution of risk.

With a constantly evolving threat landscape, cybersecurity teams, which tend to be lean, are tasked with the challenge of measuring the effectiveness of their work against a continuously moving target. They are expected to address vulnerabilities across complex systems and innovate in the age of digital transformation while trying to align cybersecurity measures with their respective company's business strategies. Because there are no widely accepted standards to measure the ROI of cybersecurity, reporting responsibilities can also overwhelm cybersecurity teams tasked with developing an effective framework for measuring outcomes.

## Filling in the gaps with cyber risk modeling

One of the greatest challenges of predicting cyber risk is the unpredictable manner in which cyber events tend to unfold. Though there is no way to fully know every single aspect of your cyber risk or which attacks your business might face in the future, a cyber risk assessment and modeling can help you more accurately estimate loss probabilities, business impact, loss distributions, and what this looks like in financial terms.




*IBM's Cost of a Data Breach Report 2022*

With properly quantified risk data, you can understand the true impact and probability of a risk. This information allows you decide where to focus your cyber investments, and how to align risk mitigation strategies with business objectives. Making calculated cyber risk management decisions means that you are less likely to over or under react to potential risk events.

**If you are at a loss with how to quantify your risk, your broker can help you in the following ways:**

- **Break down communication silos:** Your broker can help you establish a common risk language across your organization. Aligning cybersecurity and financial leaders produces more comprehensive risk data.

- **Continuously assess risk:** Working with the right broker encourages you to revisit your risk with regularity so that you are aware of how it changes in the face of a constantly evolving risk landscape.

- **Ensure access to resources:** Your broker should have access to resources that automate the risk modeling process so that it is less of a strain on your internal teams. They can also connect you to vetted, trustworthy cybersecurity vendors should you need to implement risk mitigation tools.

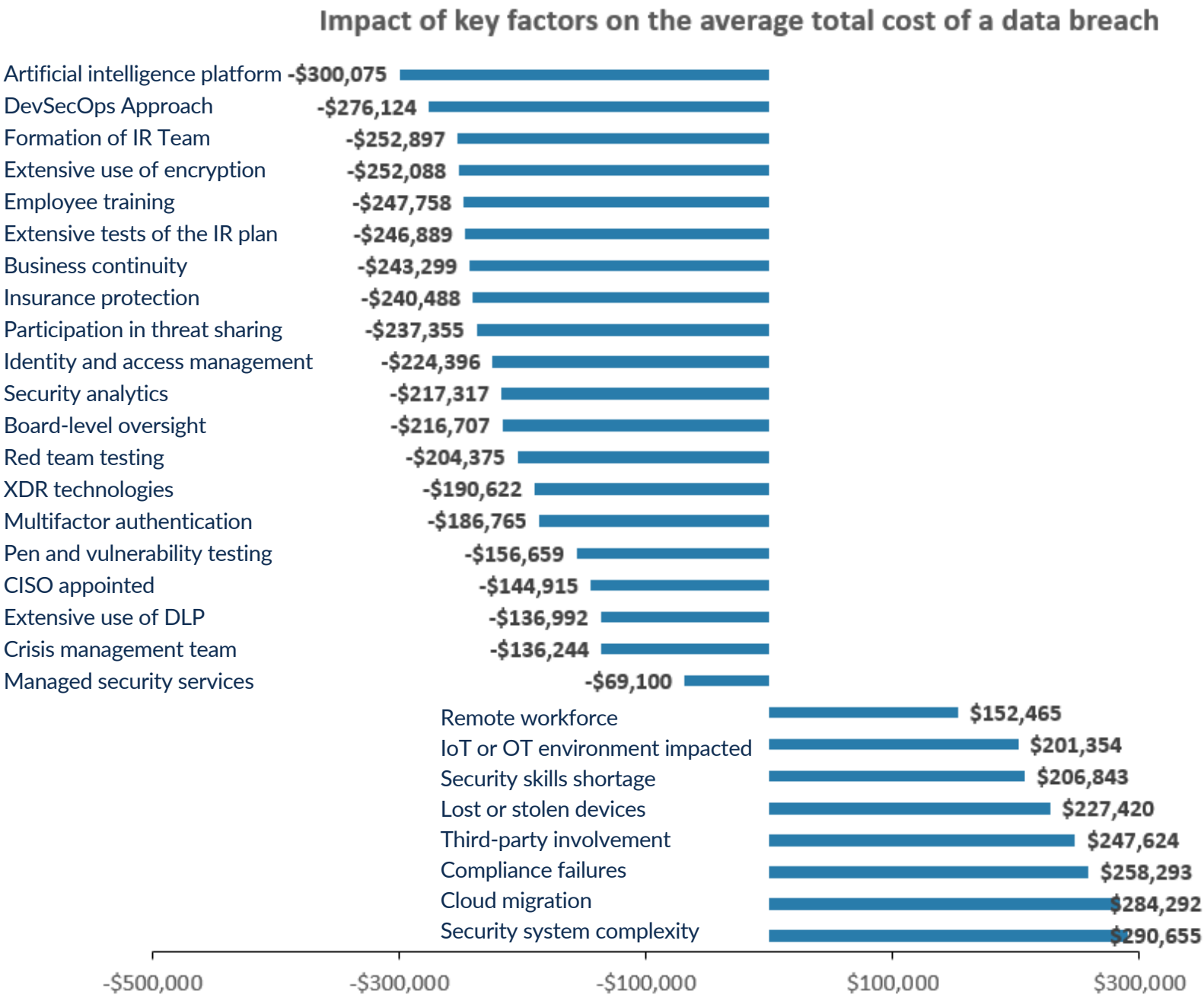
**Ultimately, data needs to be translated into a narrative so that business leaders understand the following:**

**What enables these attacks to occur?**

**What attacks are you most susceptible to?**

**How can you manage the risk through controls or risk transfer?**

**What are the financial consequences of these cyber events?**




*IBM's Cost of a Data Breach Report 2022*

# CYBER INSURANCE: A VALUABLE INVESTMENT

Unfortunately, many companies do not see the value in cybersecurity risk mitigation until they experience a data breach. In this day and age, it is no longer a matter of if you will experience a cyber event but rather when. IBM's Cost of a Data Breach Report 2022 estimates that **83% of respondents had more than one data breach**. And, according to the Netdiligence® Cyber Claims Study 2022 Report, there was no clear correlation between the size of an organization and the magnitude of a cyber-related loss. Both large companies and SMEs experienced large losses, with incidents at large companies showing 90 times more costly than those at SMEs. However, SMEs experienced what could be considered greater organizational impact at 149 SME claims with Total Incident Costs >$1M.

With the prevalence of cyber breaches, you might be wondering if cyber insurance for your business is worth it. Even though cyber coverage has gotten more expensive in recent years, it has become invaluable to those who have suffered an incident or loss.

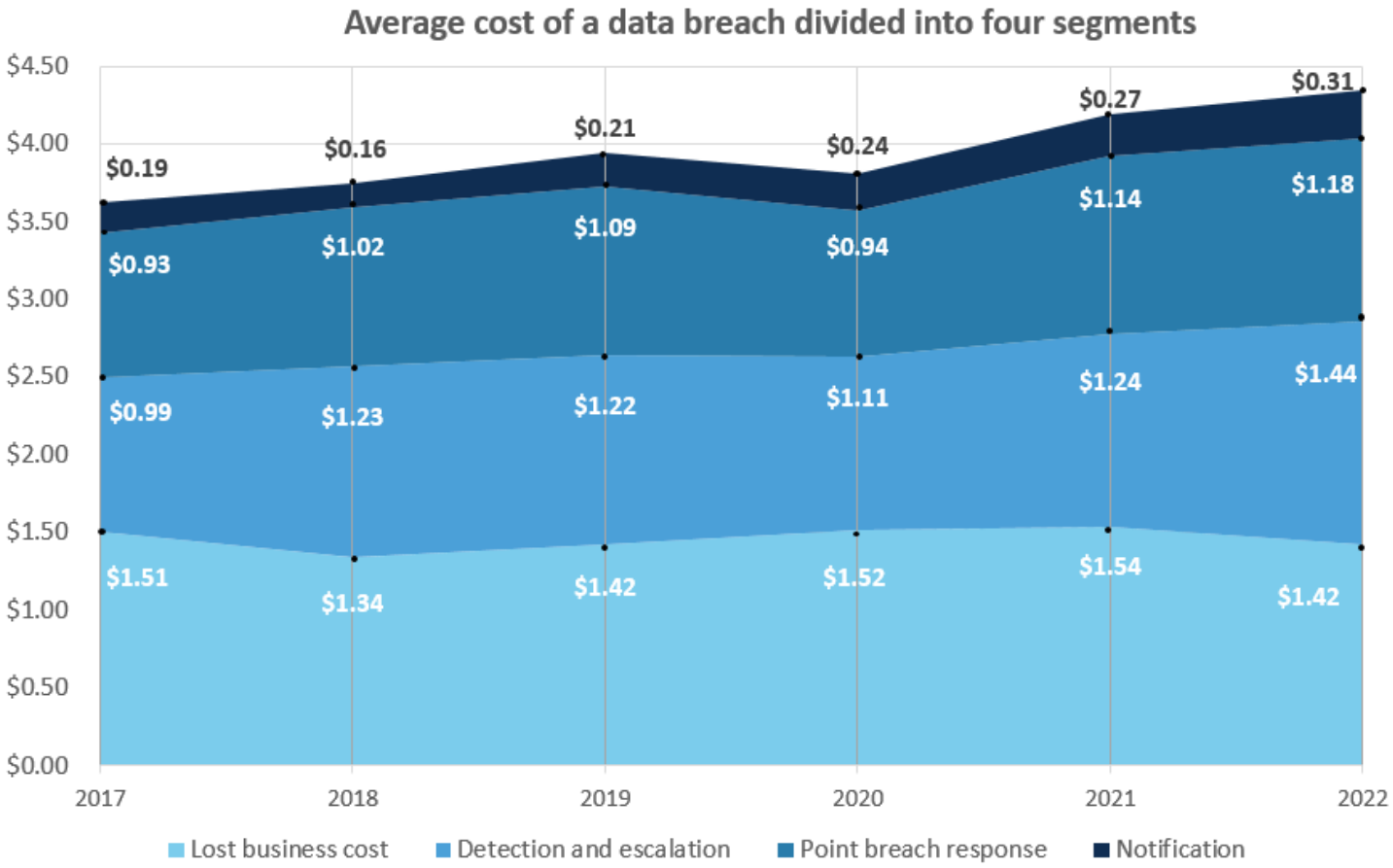
Businesses of all sizes and in all industries can benefit from cyber insurance. Any business that digitally stores data is at risk for a cyberattack. If your business does any of these, it is vulnerable to cyberattacks:

- Communicates with customers online or via voice over internet protocol (VoIP)
- Accepts online payments
- Accepts in-store credit card transactions
- Stores personal information electronically (customers, employees, and business partners)
- Transfers documents electronically
- Relies heavily on IT systems for operations

## So, why is cyber insurance a valuable investment?

If you want to offer your services to another organization, they might require you to purchase cyber coverage. If you do not have coverage, your business might miss out on opportunities to generate revenue due to an inability to fulfill vendor requirements.

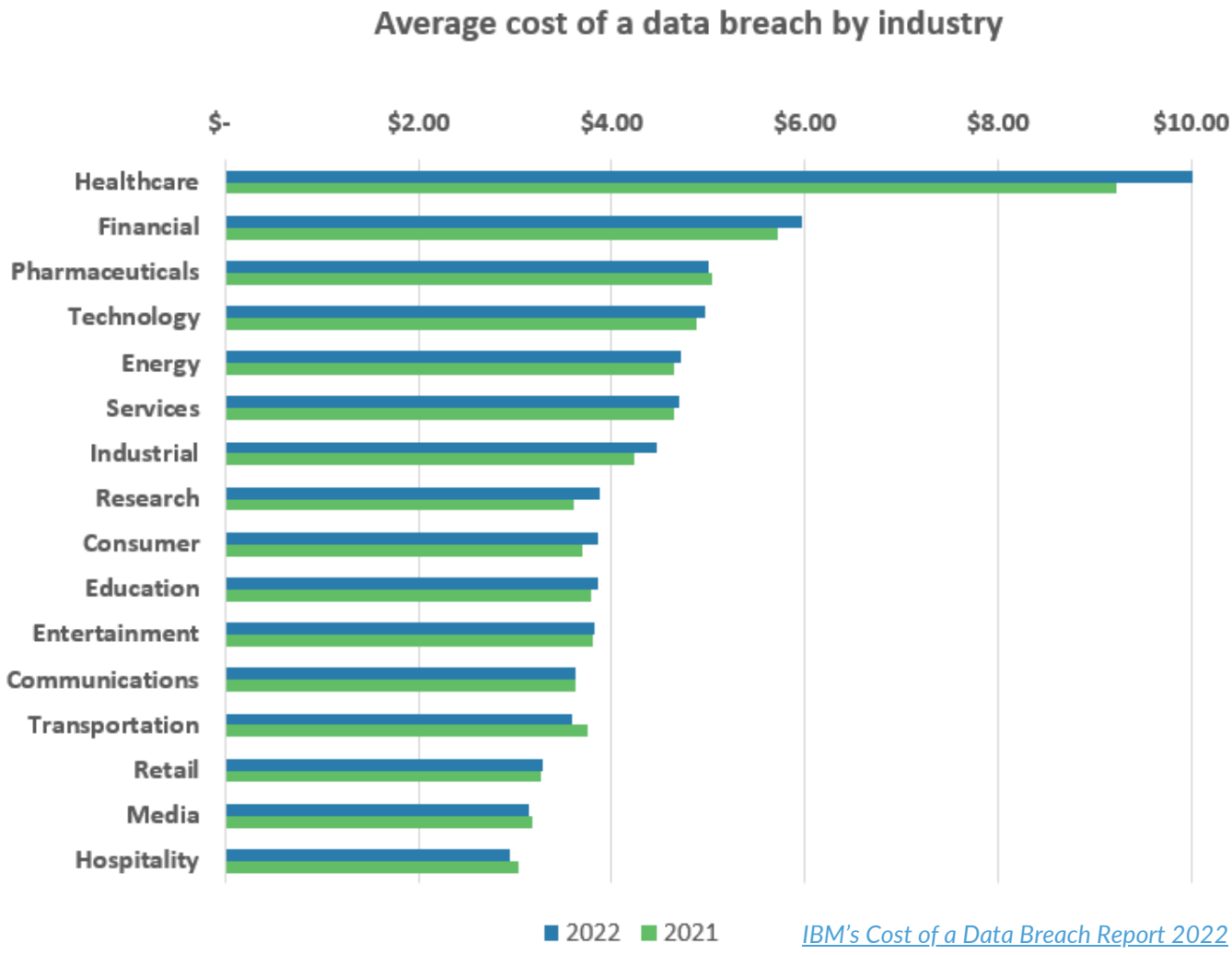
Breaches are also very expensive. A well-structured cyber policy provides financial protection from the costs that arise from a cyberattack, including legal fees, ransom payments, and data recovery. Cyber insurance can also cover the cost of providing identity protection to affected individuals, forensic investigations to determine the cause of the breach, breach containment, and remediation assistance. **Without cyber insurance, these are all things that your company would have to pay for out of pocket.**




*IBM's Cost of a Data Breach Report 2022*

Additionally, if you did not have cyber insurance, your IT team would likely have to take on the post breach cleanup, which only detracts them from the mountain of responsibilities they already have to manage on a regular basis. They might also have tunnel vision regarding what caused the breach, so an outsider's perspective provides a fresh and unbiased viewpoint about how to effectively fix the problem. In unfortunate situations when a rogue employee abused their privilege and was the malicious actor that caused the cyber breach, they have less of an incentive to fix the vulnerability correctly. **Further, insurance carriers have highly negotiated rates with top-tier incident response vendors, including privacy attorneys, digital forensic incident responders, ransomware negotiators, and public relations specialists. These firms may not entertain any business outside of their insurance carrier relationships due to bandwidth and resources.**

Though the average cost of a data breach varies by company size and industry, in 2022 the average total cost of a data breach in the United States was $4.35 million. It is easy to see why cyberattacks can be financially devastating for organizations, often forcing them to shutter their operations. Premiums vary due to many factors, but relative to the cost of an attack, the amount of an annual premium is minimal.




*IBM's Cost of a Data Breach Report 2022*

## NAVIGATING THE CYBER INSURANCE MARKET

Taking the time to understand the ROI of cybersecurity strengthens your ability to understand your cyber exposure in clear and precise terms. Continuous cyber risk quantification provides invaluable visibility into how much risk reduction you achieve with each control so that your risk mitigation efforts are both productive and proactive. **Demystifying the costs associated cybersecurity paints a clearer picture for internal and external stakeholders, such as board members, executives, and insurers so that they see the financial impact of a data breach for your organization.**

The process of obtaining insurance coverage is a practice in risk quantification on its own. Insurance carriers ask a comprehensive set of questions regarding a potential insured's controls and resources, with some minimum controls compulsory to quote. This task is arduous and requires a tremendous amount of coordination but provides feedback based upon the insurance industry's knowledge of triggers of claims activity.

When carriers understand the full scope of your cyber risk and see that you take a proactive and continual approach to understanding it yourself, they are more likely to provide more favorable terms for coverage. This is because insurers want to accurately understand the risk they are taking on and also look favorably on insureds who make cyber security a business priority. In the current cyber insurance market, finding the terms of coverage you need is more challenging than in previous years. Carriers have become extremely strict when underwriting cyber risk, which means you need to do everything in your power to understand your risk and the value of your cybersecurity investments.

## WORK WITH A QUALIFIED PARTNER

An experienced broker has a constant pulse on how the cyber risk landscape evolves and carriers' changing expectations in this dynamic environment. Our team of cyber insurance experts has connections to carriers and communicates with clients as soon as they learn of changing carrier requirements so that they can be ready to meet them. Additionally, our market reach gives us access to valuable resources that can help you quantify your risk and stay ahead of malicious actors.

# CYBER INSURANCE:

## THE UNSUNG INVESTMENT HERO

## Part 3:

*The Devil is in the Details:*
*Beware of Potential Cyber Coverage Pitfalls*

AHT INSURANCE
A BALDWIN RISK PARTNER

# The Devil is in the Details: Beware of Potential Cyber Coverage Pitfalls

*Know what your cyber policy covers and how it works when you need to use it*

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

In 2021, the FBI received about 850,000 reports of cybercrime with losses surpassing the $6.9 billion mark in the United States alone. Globally, losses in 2021 were about $6 trillion, and this number is estimated to grow to $7 trillion in 2022. With cyber threats and losses surging year over year, it is no wonder why more businesses are turning to cyber insurance for financial protection from these events.

**But buyer, beware: all cyber policies are not created equal.** Having the wrong type of coverage for your needs can provide a false sense of security that could leave your organization in a state of financial ruin if you become the victim of a cyberattack. There is no standard cyber insurance policy, which is why you and your broker need to diligently assess your cyber risk and review your existing policy. Understanding how your cyber coverage aligns with your risk profile and finances allows you to make necessary adjustments so you do not end up on the wrong side of insurance in the event of a loss.

**If you are in the market for cyber insurance or seeking to update your existing coverage, asking the following questions can help you avoid some of the common pitfalls:**

AHT INSURANCE
A BALDWIN RISK PARTNER

## DO WE HAVE CYBER COVERAGE AND/OR DO OUR CURRENT INSURANCE POLICIES COVER A CYBER INCIDENT?

**Though this question might seem like a no brainer, businesses often assume that their existing business continuity policy or property damage policy will cover a cyber incident.** This is a dangerous assumption to make because this type of policy might not cover cyber events, which would leave you financially liable should your organization experience a breach. The cost of remediation efforts and legal battles quickly add up and could detrimentally impact your business, so much so that you might not be able to recover.

Additionally, sometimes internal communication at companies is not optimal. Stakeholders might not be aware of the policies that are in place, which is why you need review whether or not you have cyber coverage.

## WHICH INTERNAL STAKEHOLDERS DO WE NEED TO INCLUDE IN THE CONVERSATION?

Cybersecurity is complex, and so is finding cyber coverage that aligns with your company's unique digital risk. Your cybersecurity IT leaders, the finance department, legal experts, and company leaders all need to continuously communicate and be on the same page about what your cyber risk amounts to and the financial exposure it creates so you can build strategies to mitigate this risk.

Determine who will be in charge of buying and selecting cyber insurance, and whose job it is to file a claim in the event of a data breach. Aligning internal stakeholders and establishing accountability helps ensure that your business is managing and mitigating cyber risk. It is also important to consider who will be involved in the event of a claim or cyber incident. Time is of the essence at the time of an incident and knowing who needs to be in the room is a critical part of any incident response planning. Carriers look favorably upon insureds with a culture of cybersecurity, as preparedness minimizes the probability of a loss.

## ARE WE ABLE TO MEET THE REQUIREMENTS FOR COVERAGE?

Over time, cyber carriers have increased the prerequisites insureds need to meet to obtain coverage. When you apply for coverage, you will need to answer the carrier's questionnaire so that they know the technology your company uses, the cybersecurity measures you have in place, the coverage you might need, and the limits they can offer.

Though this list is non exhaustive and different cyber carriers have different requirements for coverage, most of them will want to see that you have these measures in place before providing coverage:

- Employee awareness trainings and phishing simulations
- Multi-Factor Authentication (MFA) for all users
- Password manager utilized across your user base
- Frequent and replicated back-ups
- Back-up testing
- A principle of least privilege policy
- Use a Virtual Private Network (VPN)
- Secure Remote Desktop Protocol (RDP)
- Encrypted backups
- Removal of end-of-life (EOL) and end-of-service life (EOSL) devices and software
- Endpoint detection & response (EDR) solution to monitor and stop suspicious activity
- Enable and analyze logs for your devices and digital landscape
- Patch management program
- Continually tested incident response plan

## WHAT DOES YOUR CYBER POLICY COVER?

The cyber insurance you purchase should be based on your identified areas of risk and mesh with your overarching cybersecurity strategy. Having the right policy in place can make a huge difference should you experience a cyberattack. A cyber policy that aligns with your risk provides support and resources that make it easier to manage a crisis so that your business can recover. Working with a trusted broker helps ensure that you have the right coverage and are well prepared to manage a cyber event.

In the event of a breach, your business might require resources and tools to respond to the incident but may also require defense in the event that third parties suffer a loss.  A comprehensive cyber insurance policy includes first-party coverage and third-party liability.

Similar to commercial property insurance, first-party cyber liability insurance helps protect your company by responding to data breaches at your own business. If your business relies heavily on IT systems to operate and stores sensitive data, such as credit card information and personal information, you need this coverage.

**First-party liability can cover the costs of:**

- Communicating with impacted customers
- Credit monitoring
- Forensic analysis to identify the source of the attack
- Data restoration
- Public relations and reputation management services
- Losses due to ransomware, cyber extortion, etc.
- Expenses for remediation activities
- Loss of income
- Other recovery activities

If a client shares its sensitive data with your business, they expect you to keep it safe. Third-party liability coverage is designed to provide financial protection for your business if you fail to prevent a data breach at a client's business. Much like professional liability insurance, it can provide protection if another company sues you for compromising their data and causing losses or damages to that company.

**Third-party coverage can help pay for:**

- Legal fees
- Government penalties and fines
- Cost of responding to regulatory inquires
- Settlements and judgments related to the claim

Always remember that even though first and third-party liability coverage can cover these costs, you need to carefully review the details of your coverage to know what exactly your policy covers. Cyber policies are not standardized, so the coverage for events can vary greatly across carriers. When you review areas of coverage, zero in on exclusions that could increase your liability in the event of a loss.

## ARE THERE COVERAGE EXCLUSIONS WE NEED TO BE AWARE OF?

You do not want to end up in a position where you assumed your insurance would cover the costs of an incident only to learn that it is excluded in your policy and that you will have to pay to remediate the breach. Policy wordings and definitions are inconsistent, with some policies clearly stating inclusions and exclusions, and others not being very explicit in what they do and do not cover.

**Though you might be able to purchase an endorsement that could provide coverage, many carriers exclude or severely limit coverage for the following events:**

- Consumer protection acts
- War and terrorism
- Contractual liability
- Electrical or mechanical failure
- Infrastructure breaches or failures
- Voluntary shutdown coverage
- Regulatory fine limitations
- Loss at an associated company not explicitly listed in policy

## DO WE HAVE THE RIGHT AMOUNT OF COVERAGE?

To avoid coverage gaps, you need to quantify your cybersecurity risk. Quantifying your risk helps you determine what you need to do to improve your cybersecurity, and how to best structure a cyber policy for your specific risk profile so that you do not over or under insure. Placing a dollar amount on your cyber risk is challenging, but your broker can provide resources that can help with the risk quantification process.

**Coverage gaps may occur if:**

- You assume that a standard business loss policy will cover a cyber loss
- The base retention is high, and a loss is not covered if it exceeds that mount
- You waive coverage for direct damages or incidental damages
- You choose coverage limits that are too low for your risk

## CYBER INSURANCE: THE UNSUNG INVESTMENT HERO

Read Part 1: Quantifying Cyber Risk & Proving the Value of a Cyber Insurance Investment

Read Part 2: Understand the ROI of investing in Cyber Insurance

## HOW DOES THE CARRIER RESPOND IN THE EVENT OF A CLAIM?

If you do get hit with an attack and need to use your cyber policy, how a carrier responds to your claim is extremely important. Your carrier will require you to follow specific steps and meet the criteria in your policy prior to paying out a claim. You need to familiarize yourself with your policy before the need to make a claim arises.

**Here are some things to keep in mind:**

- Review your policy at renewal so that you meet any updated requirements. If you have not complied with these updates, a carrier may deny your claim.
- Most carriers have a specific panel of vendors that must be utilized for a claim to be paid in full
- Know the reporting time requirements for your insurer and abide by them. Inform your carrier about an incident as soon as you can (within their reporting time parameters).
- Be aware of the carrier's reporting requirements for a cyber incident.
- Look at how restrictive trigger language within the policy is and if it impacts how a carrier will respond to your claim.
- Determine if your policy has "pay on behalf of" language, or if you will have to cover the costs of a breach upfront before getting reimbursement. If you have to pay for remediation efforts with your own funds and wait for reimbursement, this could be extremely inconvenient and have a severe, negative impact on your organization's balance sheet. "Pay on behalf of" language decreases the financial inconvenience of a cyber event. Cyber policies have certain coverage parts that require reimbursement to the insured, such as cyber extortion (ransomware) payments.

## DOES THE CYBER CARRIER UNDERSTAND YOUR INDUSTRY'S RISKS?

Though there might be overlap in cyber risk across industries, certain lines of business have particular areas of cyber exposure that are unique to their operations. At a baseline, your cyber carrier needs to fully comprehend the dangers that wide-ranging cyber threats pose to your enterprise. In addition to this, work with a broker that has experience in your industry. For example, if you are a healthcare company, your broker will help the cyber carrier comprehend the privacy and security requirements that HIPAA imposes on, as well as the privacy concerns of sharing, patient data. Or, if you run a manufacturing operation, you want your broker to ensure the cyber carrier has a grasp on the supply chain cyber exposures your business faces.

## FIND THE RIGHT COVERAGE IN A HARDENED CYBER INSURANCE MARKET

The demand for cyber coverage has grown faster than market capacity, which is why it is now harder than ever before to find and place coverage that meets an organization's needs. With underwriting scrutiny at an all-time high and carriers providing less favorable terms for coverage, you need to work with a team of experts capable of navigating a hardened cyber insurance market. Our team can help you understand what your cyber policy covers and enhance it for your unique needs as they continue to evolve.

Contact us to learn more about how we can help you get the coverage you need.

# CYBER INSURANCE:

## THE UNSUNG INVESTMENT HERO

## Part 4:

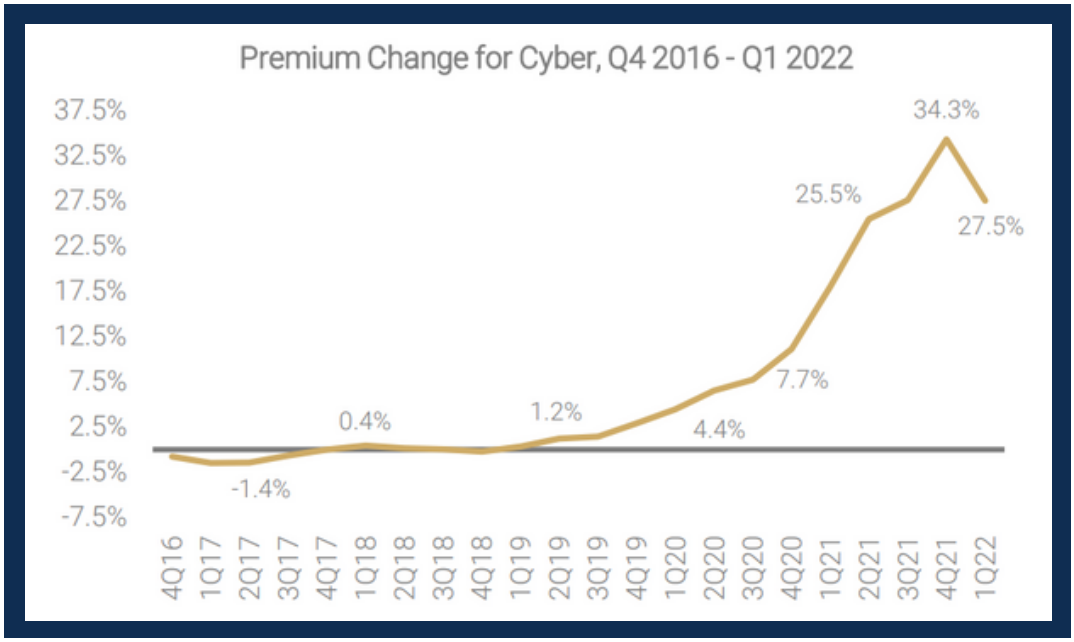
*Not All Brokers Are Created Equal: Importance of Investing in the Best Partner for Placing Cyber Insurance*

AHT INSURANCE
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




CIAB Commercial Property/Casualty Market Index 2022

AHT INSURANCE
A BALDWIN RISK PARTNER

**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 if 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 you're 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.

# CYBER INSURANCE:

## THE UNSUNG INVESTMENT HERO

AHT INSURANCE

A BALDWIN RISK PARTNER