CYBER INSURANCE:

THE UNSUNG INVESTMENT HERO

Part 2:

Understand the ROI of Investing in Cyber Insurance

Burnham | WGB

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.

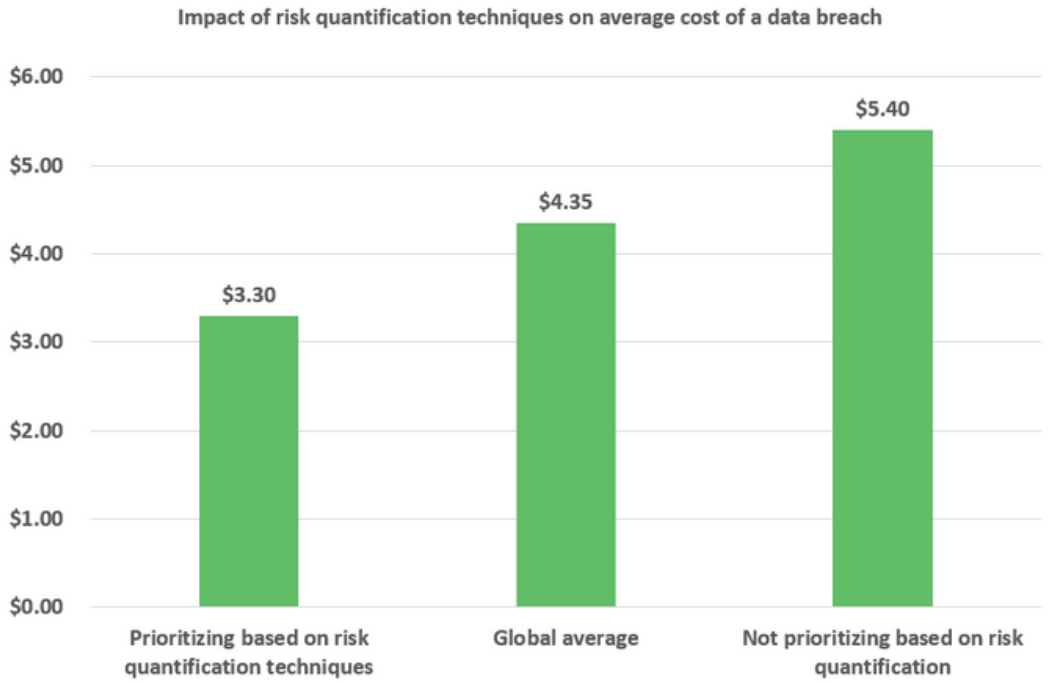
CHALLENGES: DEMONSTRATING THE VALUE OF CYBER RISK MITIGATION INVESTMENTS

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

Understanding the Impact of a Risk Event

With properly quantified risk data, you can understand the true impact and probability of a risk. This data helps you decide where to focus your cyber investment, 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.

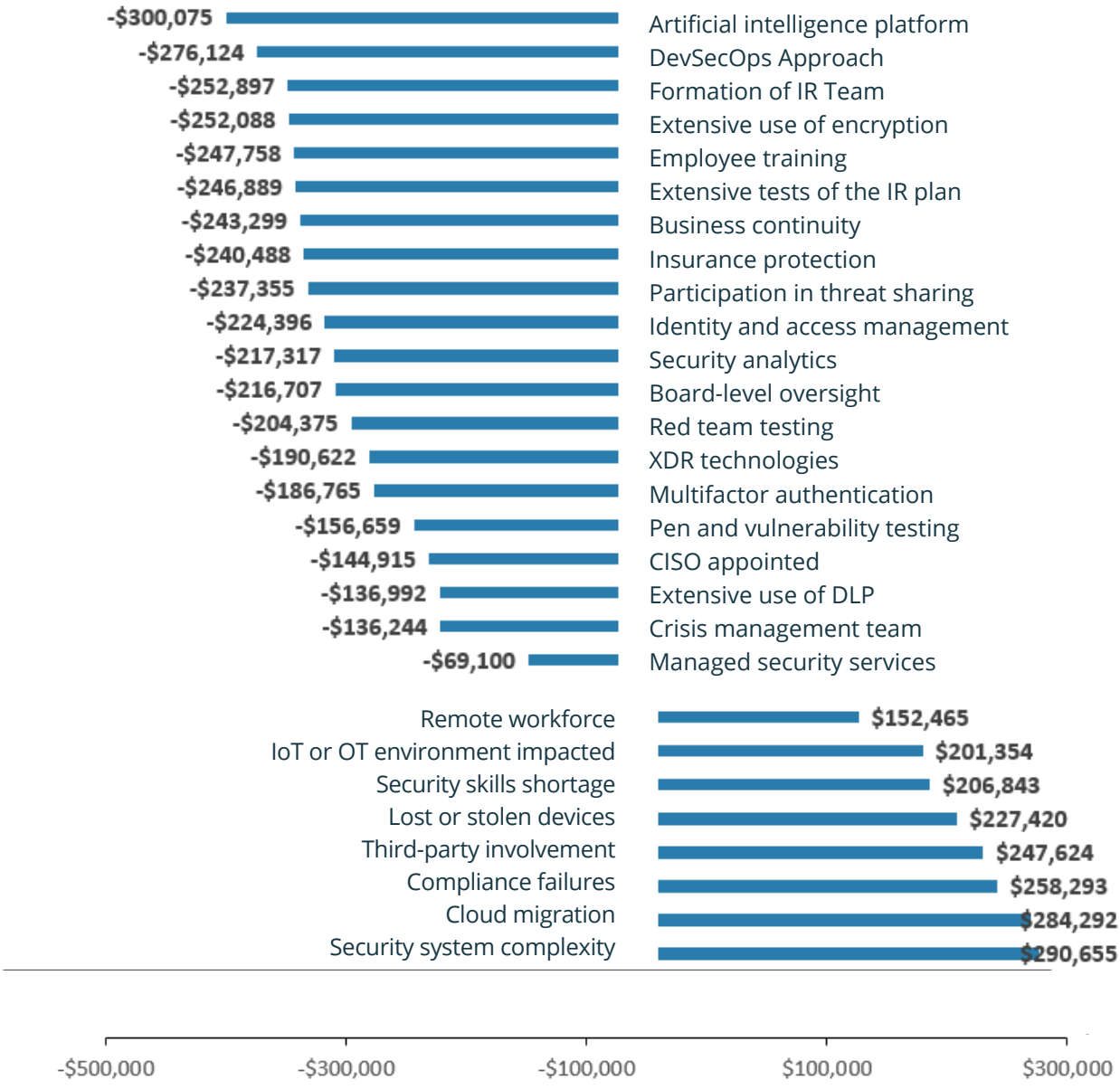
If you are at a loss with how to quantify your risk, your broker can help you in the following ways:

- **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?**

Impact of Key Factors on the Average Total Cost of a Data Breach



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.

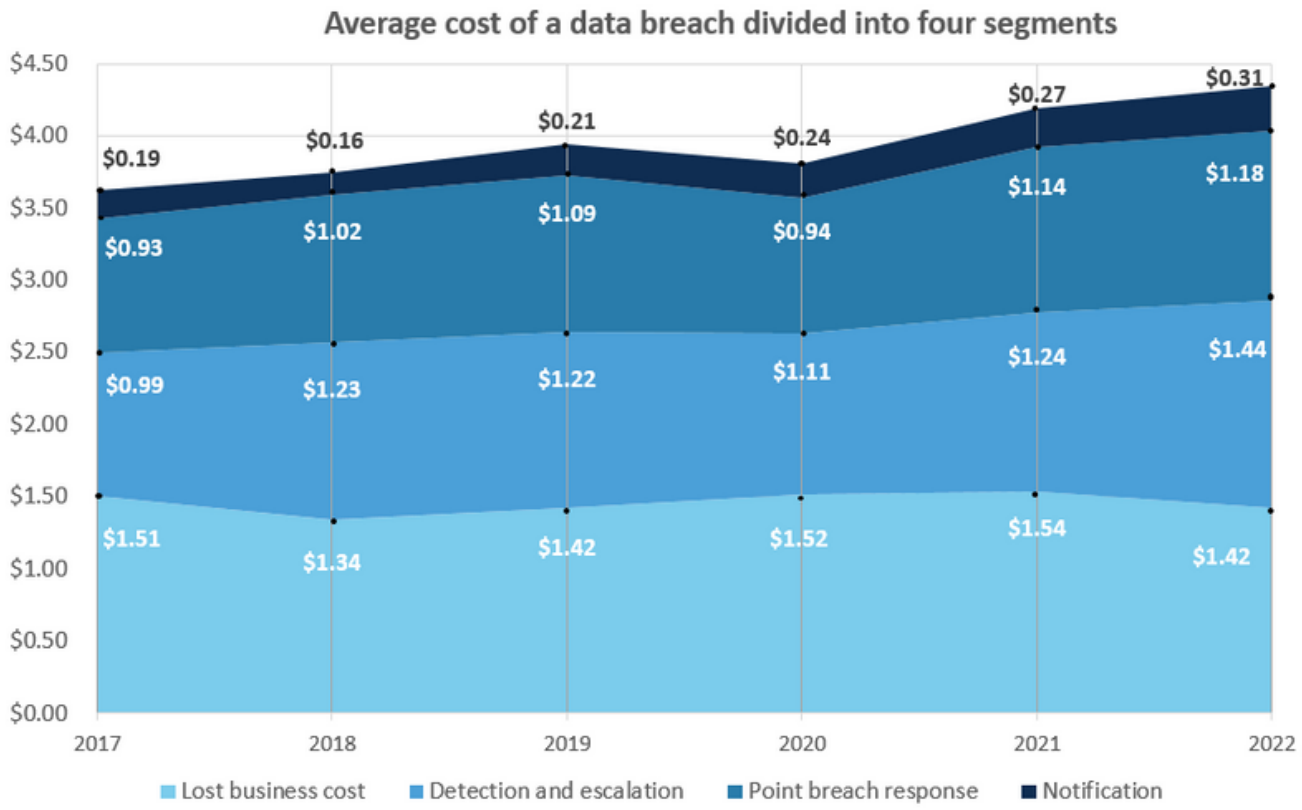
Businesses of all sizes and in all industries can benefit from cyber insurance. Any business that digitally stores data is at risk for a cyberattack. If your business does any of these, it is vulnerable to cyberattacks:

- 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 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.

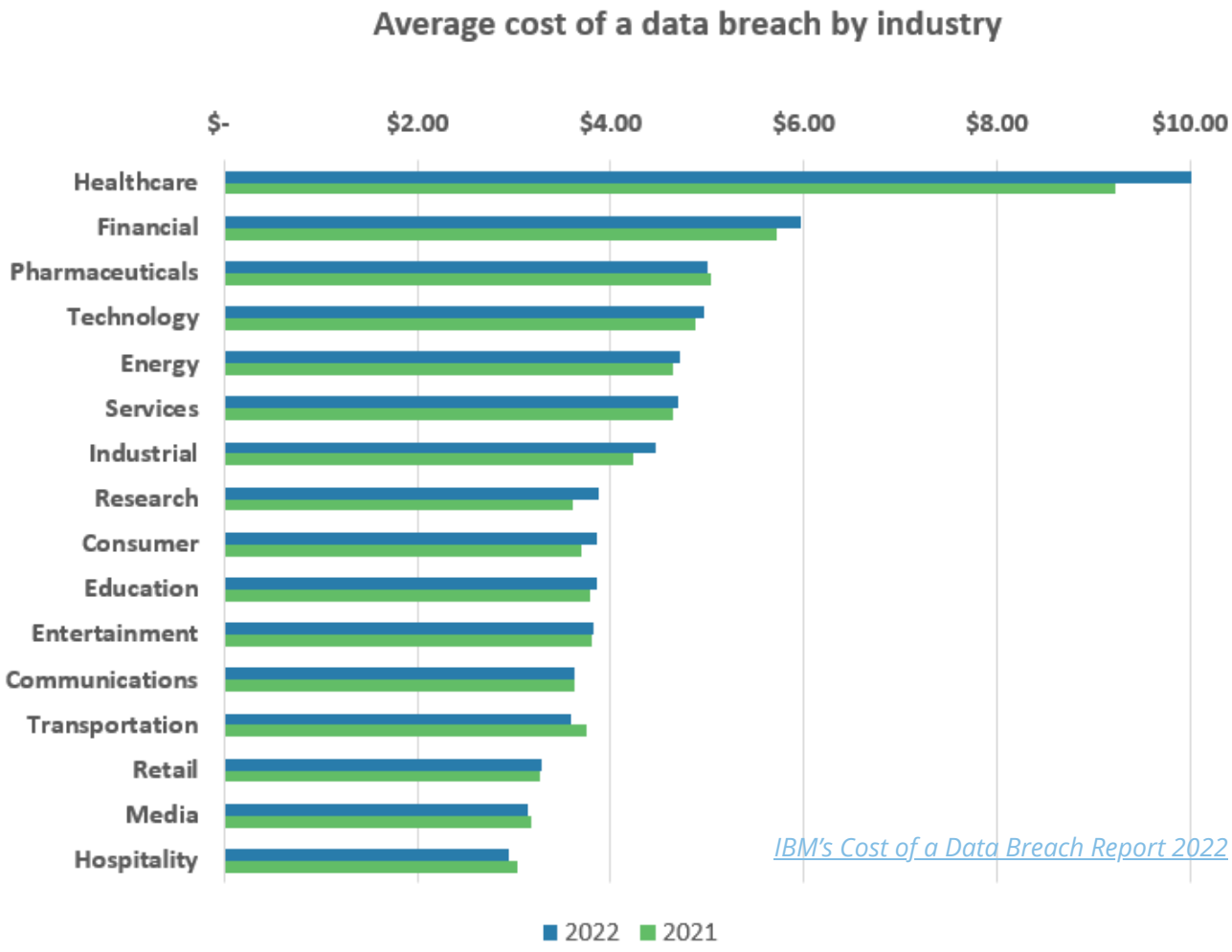
Breaches are also very expensive. A well-structured cyber policy provides financial protection from the costs that arise from a cyberattack, including legal fees, ransom payments, and data recovery. Cyber insurance can also cover the cost of providing identity protection to affected individuals, forensic 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 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.

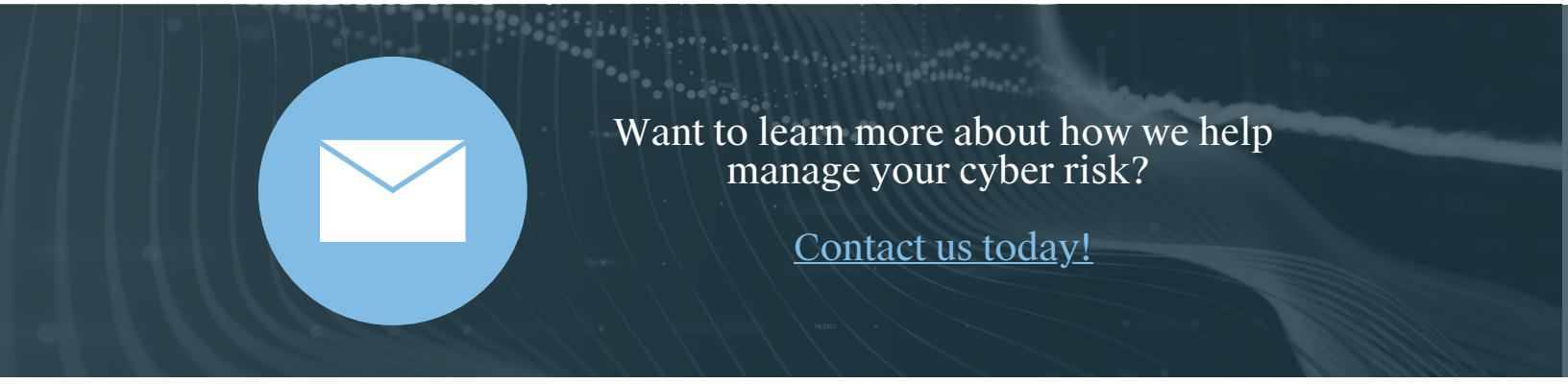
DON'T OVERPAY FOR CYBER COVERAGE

Get the Right Cyber Coverage at the Right Price

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.



Burnham | WGB
A BALDWIN RISK PARTNER

Powered by Baldwin Krystyn Sherman Partners Insurance Sales, LLC
DBA Burnham WGB Insurance Solutions | CA Insurance License 0F69771

CYBER INSURANCE:

THE UNSUNG INVESTMENT HERO

Burnham | WGB

A BALDWIN RISK PARTNER