CYBER INSURANCE:

THE UNSUNG INVESTMENT HERO

Part 1:

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

BRP

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.

BRP

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.

BRP

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 decision makers 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:

- 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.

BRP

CYBER RISK AND CASH FLOW MANAGEMENT

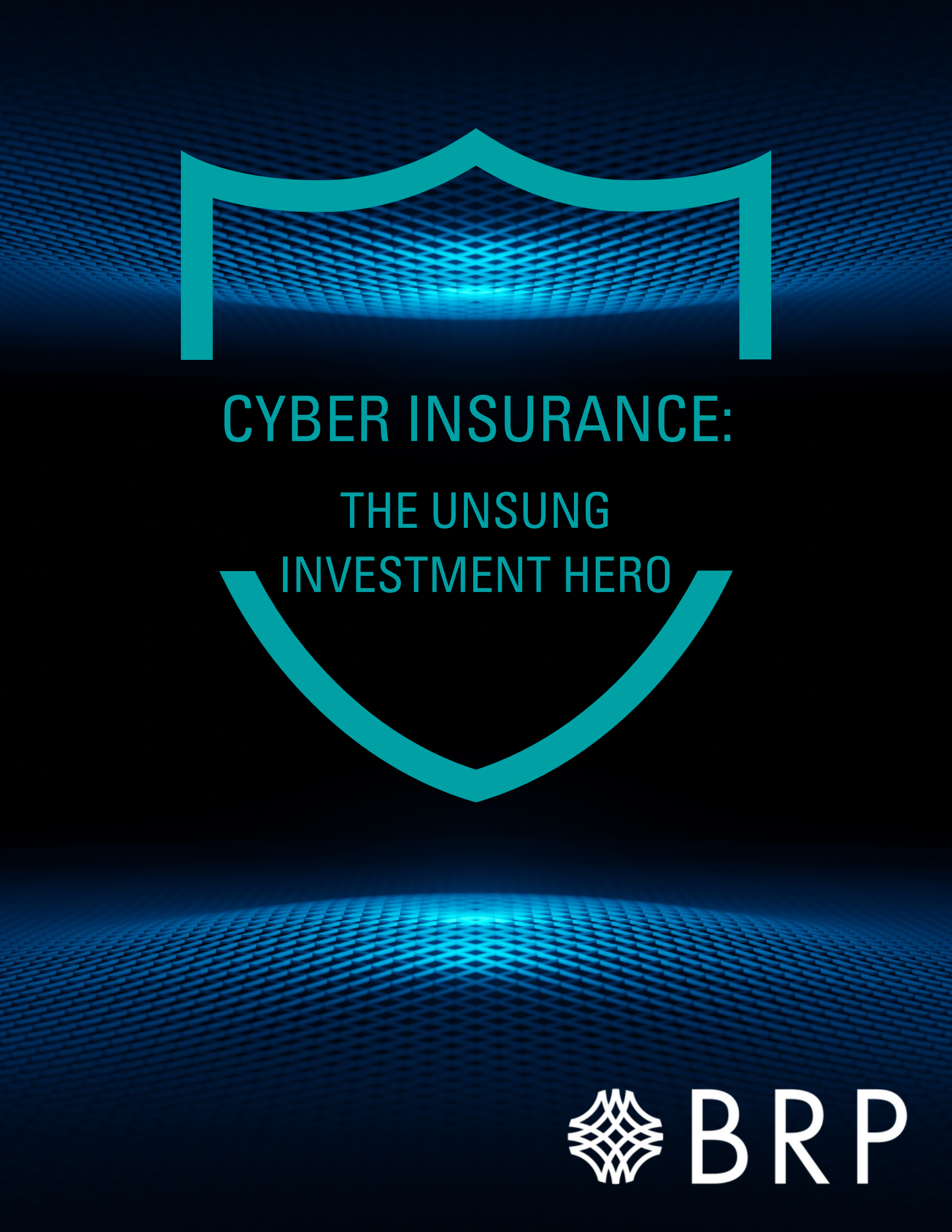
Organizations need to understand how their cybersecurity posture correlates to business consequences and be prepared to rebound in the event of a cyberattack. A successful attack can cause devastating financial disruption for your business or even shut it down, which is why they are one of the top risks 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.

BRP



CYBER INSURANCE:

THE UNSUNG INVESTMENT HERO

BRP