CYBER INSURANCE:

THE UNSUNG INVESTMENT HERO

Part 3:

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

Burnham | WGB

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, the questions that follow can help you avoid some of the common pitfalls.

DO WE HAVE CYBER COVERAGE 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 this coverage.

WHAT DOES YOUR CYBER POLICY COVER? (CONT.)

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:

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

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 panel of vendors that must be used 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?

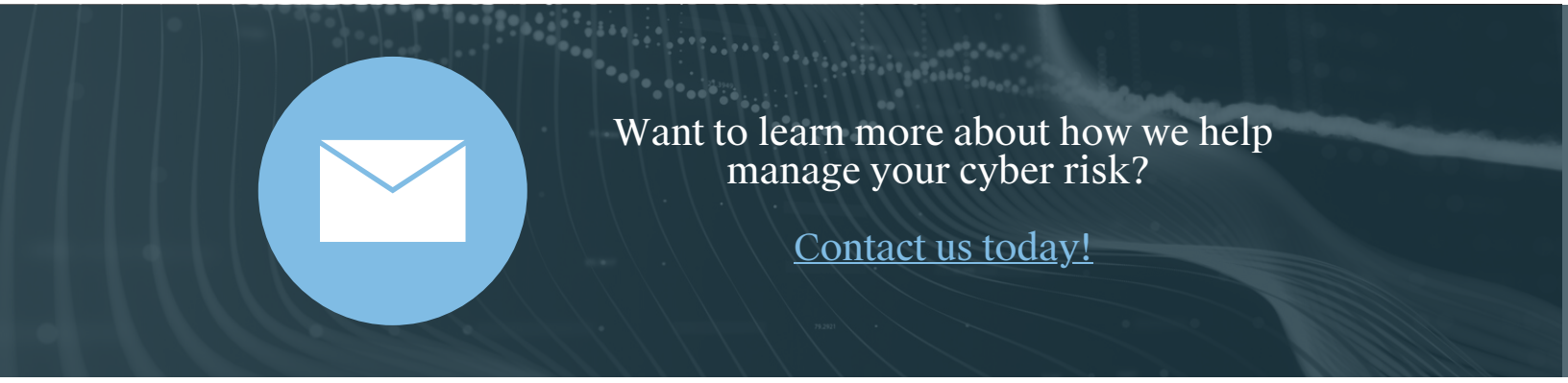
Though there might be overlap in cyber risk across industries, certain lines of business have particular areas of cyber exposure that are unique to their operations. At a baseline, your cyber carrier needs to fully comprehend the dangers that wide-ranging cyber threats pose to your enterprise. In addition 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.

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