nuspire | 221b CONSULTING

A CISO's Guide to Cyber Insurance

nuspire.com

221bconsulting.com

Table of Contents

Introduction

The modern insurance story began in the 17th century. After conducting a risk assessment, an insurer provided coverage for ships carrying goods to their destinations. Skip ahead to the last 20 or so years, and we see that insurance policies (including cyber) still involve insurable events and risk calculation. Initially cyber coverage piggybacked on other types of insurance policies (making it a bit of a "Frankenstein" patchwork of options). Now standalone cyber policies are the norm.

But over time, cyber risk has changed. The first major hack of a retail store and subsequent mainframe breach upended the industry. CISOs are in a precarious position in light of the potential consequences of threats such as ransomware and denial of service (DoS) that can take down a business.

Failure to purchase cyber insurance intensifies risk exposure. No balance sheet can protect a business from lawsuits, attorney fees, restoration costs and reputational damage. Cyber insurance now is a business necessity, and organizations need to get cyber insurance coverage as right as possible. The optimal way to do this is for CISOs to collaborate with risk managers and bring probability thinking and cybersecurity maturity into the discussion.

This guide helps CISOs be smarter about cyber insurance and risk management. In it, we share lessons learned, best practices and more:

- The purpose of cyber insurance
- Cyber insurance industry insights
- Insights into coverage
- Industry trends
- Tips to streamline insurance purchase
- CISO recommendations
- Important cyber insurance terms

Chapter 1.

Why Is Cyber Insurance Complicated?

The current environment feels a bit like whack-a-mole. Enterprises are purchasing cyber insurance at record levels to help limit costs associated with cybersecurity incidents. Many aspects of the industry are in flux, as is the threat landscape. The cyber insurance process, whether for initial purchase or renewal, is perceived by many as opaque and intricate. Underwriting is evolving as insurance carriers refine coverage terms. Rates are going up, which puts pressure on buyers to spend dollars wisely.

The number of written cyber insurance policies in force increased by 21.3% from 2019 to 2020.[1]

Persistent and increasingly sophisticated bad actors continue to assault organizations, ratcheting up uncertainty and risk. Security controls vary across companies and industries. Risk assessment activities – essential to identifying the right amount and type of coverage – are changing as more stakeholders weigh in with questions and concerns.

Lack of clarity, risk and security silos and the decision process top our list of complicating factors.

Lack of Clarity

How does the cyber insurance industry work? The words *ambiguous* and *obscure* come to mind. Cyber insurance terms are dense. Forms can be difficult to understand and claims difficult to file. Policies lag the market, contributing to potential risk-coverage mismatches. Insurance companies may or may not pay claims based on underwriting nuances. For example, ransomware coverage was included in the past, but now it may be sublimited (application of a payment cap).

The frequency of cybersecurity incidents is at an all-time high. Research shows a 68% increase in data breaches over 2020, and that 10% of breaches involve ransomware – double the 2020 figure.

Source: IBM, Cost of a Data Breach Report, 2021

79% of survey respondents say they've encountered ransomware attacks, and 35% admit one or more of those attacks led them to lose access to data and systems.[2]

Additionally, gaps in coverage are common because cyber insurance terms and conditions vary from one insurance carrier to another. Risk typically is spread among multiple carriers resulting in a tower of coverage. If each carrier provides $5 million or $10 million, for example, five to 10 carriers are providing an aggregate $50 million program. Are the carriers and policies in the tower aligned? Is the primary carrier the lead decision maker on claims? How are claim decisions made? The answers may be different in every case.

[1] NAIC, Cyber Insurance Report, October 2021
[2] Splunk, The State of Security 2022

Risk and Security Silos

Security technologies and cybersecurity services are key to cybersecurity maturity, which leads to more favorable cyber insurance outcomes. In many organizations, however, security controls play a large but underserved role in cyber insurance decisions.

Risk and security managers tend to operate independently. The teams aren't leveraging collective knowledge and resources. And when risk and security teams aren't communicating, issues begin to fester, problems that aren't really problems receive attention and opportunities are lost or overlooked.

Consider this scenario. A risk manager doesn't provide a CISO with a summary of the primary terms and conditions of a policy. The CISO believes there is applicable coverage for the majority of events. The result? The organization is underinsured for certain events.

Or this scenario. A CISO fails to provide continual updates on threat vectors to a risk manager. The risk manager may place insurance or attempt to negotiate improved terms and conditions in an area of coverage that isn't a primary threat to the organization. Now the organization is over insured for one risk and underinsured for a greater threat. And, the risk manager loses negotiating leverage due to an incomplete risk analysis.

Fortunately, the silos are beginning to break down as CISOs and risk managers recognize they need each other, and that collaboration is the way forward to improve risk assessment, identify worst-case scenarios and apply probability thinking – all fundamental activities to improve cyber insurance outcomes.

Probability Thinking.

The reasoned chances of success associated with different types of cyberattacks and calculation of related consequences to the business.

The Decision Process

Risk managers take the lead on the lengthy, elaborate cyber insurance process by:

- Analyzing all types of risk including financial, operational, information security, legal and so on
- Matching scenarios to cyber insurance coverage to recommend limits
- Determining to what extent executives and board members may be decision influencers related to insurance placement and security controls
- Determining if the insurance premium is so expensive it is a net negative scenario
- Discussing alternatives if certain must-have controls required to obtain coverage also result in a net negative

In addition, organizational leaders are raising important questions that expand scope and bring more voices to decision-making.

FINANCE AND RISK MANAGERS	LEGAL AND OPERATIONS MANAGERS
• What is our security program? • How does it affect insurance coverage? • How are we measuring security effectiveness? • How can we strengthen cybersecurity?	• What are known perceived deficiencies? • Are they high-undertaking, low-value propositions? • Are they prioritized in some manner? • Will they impede or impair operations?

As time passes, the decision process involves more data gathering, more variables, more influencers, more compromise.

Technical transparency is important all the way up the organization to board members, who have a fiduciary duty to protect data and the business. In the past, the company typically was sued. Now, the company, executives and board members often are pulled into lawsuits.

Should you put a CISO or CIO on the board? If you do, the level of fiduciary duty rises. It may be better to have an arm's length relationship in which board members are conversant about security controls but rely on the CISO's or CIO's expertise. Also, it's critically important for CISOs and CIOs to communicate in language the board members can understand and act upon. Avoid technical jargon and acronyms as much as possible.

Chapter 2.

Cyber Insurance Technical Considerations

Imagine two organizations. One has advanced security controls like multifactor authentication (MFA), privileged access management (PAM) and encryption. One has none of these controls and lax password policies. An organization that's more cyber mature should pay less for cyber insurance than a low-maturity organization, right? Yes, but we veer into complexity again.

The must-have and nice-to-have security controls vary by industry and organization, making it difficult to develop standardized baseline protection. And, organizations and insurance brokers/carriers typically have little ability to measure the effectiveness or accuracy of security controls.

Technical Control Over Probability

Security controls are chosen to reduce the probability of successful attacks and incidents. But probability is a moving target. Enterprises buy security technology in three- to five-year cycles. The bad guys adapt in months. CISOs can't expect the board to approve additional spending on new or different controls every few months. But you can take steps to swing the odds in your favor.

Keep an eye on controls and make sure they are functioning properly. Monitor your threat environment continuously and communicate up the line when you see emerging threats, such as title/ownership theft, crypto, blockchain and NFTs, which represent an entirely new dimension of cybersecurity. Start planting seeds now about the future need for defenses that don't yet exist.

A Word About Bitcoin and Ransom Payments

Be aware of Department of Treasury regulations about not financing terrorism by paying ransoms. Some business leaders are concerned about being held liable for facilitating terrorist activities if they pay ransoms.

Keep in mind that your organization typically isn't the ransom payer. You don't have the expertise to negotiate with hostage takers. Don't set up a bitcoin wallet because you won't know ahead of time which cryptocurrency a bad actor wants or even if the actor will accept bitcoin. Wallets can be found and compromised.

Your risk manager can seek guidance from your broker and carrier to navigate the ransom decision and help your organization stay out of trouble. Carriers aren't going to act in a way that puts their organizations – or yours – at risk.

Technical Nuances in Action

The following scenarios illustrate just two of many situations in which technology influences decision maker thinking, insurance underwriting and policy payouts.

Scenario 1. Buying Technology to Address Compliance

Many security leaders satisfy compliance requirements by implementing technology, and they assume that these controls make them more secure. But compliance doesn't equal security or security maturity. For example, to meet PCI requirements for securing credit card information, an organization may segment only credit card information on the network. This allows an assessor to check the box, but what about sensitive employee and customer data that is scattered around the business?

Know where all of your organization's sensitive data is located and apply appropriate security controls. The finite details of implementation matter so you can measure and confirm over time the effectiveness of MFA, PAM, encryption or other controls. Can you say yes when the carrier asks if the encryption applied to a particular database actually encrypts customer information? If you can't, and something bad happens, the anticipated cyber insurance payout may be withheld.

Scenario 2. Bolstering Incident Response

Incident response capabilities are core aspects of security maturity and, in turn, favorable cyber insurance terms. Many organizations have invested in pre-incident detective and preventive technologies such as firewalls, antivirus, MFA and behavioral analysis. But post-incident response proves challenging for many.

Why are response tools important? Waiting periods. Let's say a business discovers an attack but lacks response tools such as forensics and threat hunting to investigate the incident and devise a rapid recovery strategy. An organization may be on its own for 24 or 48 hours to contain a threat and get up and running again. You can't afford delays when factory systems or healthcare devices or other critical systems are down.

Make sure you have tools in place to respond to incidents and determine after the fact what happened. Build an incident response toolkit with:

- A reliable backup solution
- Tested restore capability – particularly important if ransomware has locked up your systems and data
- Threat hunting tools – to look for indicators of compromise such as outbound command and control connections
- Digital forensics tools to grab malware samples, submit them for analysis to the insurance carrier's incident responder and understand if a breach is reportable

Digital Forensics and Breach Reportability

A retail store's point-of-sale (POS) system is compromised by malware. The suspected target is credit card numbers whose theft must be reported. Malware analysis shows the target is electronic health records, which do not require disclosure. Now you know there's no need to disclose a credit card breach to the acquiring bank (payment processor) or customers.

Continuous Security Improvement

Security controls need to evolve to show continuous improvement, which insurance carriers consider during underwriting. Prior nice-to-have controls may now be controls you must have just to receive a quote. To determine which controls are most important in your organization, start by understanding your threat vectors and high-priority industry-specific threats.

Additionally, insurance carriers have resources to assist your organization with continuous improvement. Carriers have access to many other clients and can talk to your risk manager about the most critical security controls in your industry and about emerging threats. These mutually beneficial conversations can increase protection for your organization, which in turn reduces carrier exposure. It's likely that must-have controls will include:

- Multifactor authentication
- Biometrics
- Controlled access privilege
- Privileged user review
- Network segmentation/micro-segmentation

Tech alone isn't the answer.

It's how tech is implemented and who is monitoring it and making sure it's working properly in the right places.

Chapter 3.

Key Cyber Insurance Trends and Their Business Impact

Keep an eye on certain trends because they help define the context in which risk assessments and decisions are made by both insurance buyers and insurance carriers.

Market Corrections and Market Shifts

A market correction generally happens every two or three years due to multiple, large industry claims, or a change in exposure or other variables such as a low interest rate environment. Insurance companies not only write cyber policies but also property and casualty (P&C) policies and other lines. They look holistically at their books of business and how to rebalance them. In underwriting meetings, a carrier may suggest that a policy is specific to your business and only for cyber. This is true to some extent. But if the carrier's P&C business is down, revenue needs to be made up elsewhere. Likewise, if the cyber line is hard hit, cyber insureds will be hard hit as well. Think of siblings in a family. None are treated completely independently when it comes to discipline.

A market shift occurred in 2019. Prior to 2019, cyber insurance coverage was fairly broad. It has narrowed considerably, and we're not likely to see a return to those terms anytime soon, if ever.

Underwriting Evolution

Underwriting has changed significantly in recent years. Underwriters used to ask, “Do you have a CISO?” Now, underwriters assume an organization has a CISO, and they go deeper. The first question might be about reporting structure. While underwriters understand that CISOs commonly report to a CIO, they recognize potential conflicts. CIOs drive revenue growth, and CISOs protect assets.

Underwriters scrutinize CISOs and their teams to determine horsepower and bench strength in case of a CISO departure. If an underwriter isn’t comfortable with who steps in to replace a departing CISO, the premium will likely go up. Be prepared to discuss the following:

- CISO’s educational background, credentials and certifications
- Security industry experience separate from CISO positions
- Team backgrounds and experience

Underwriting practices push precision and adaptability into the security decision-making process. In the past, companies typically had a single security program with a single leader who deployed processes and technologies for the entire business, although some very large companies had security programs within divisions. Working with budgets that are always finite, CISOs now need to be more precise about defending the assets that are most likely to cause financial loss if something bad, like ransomware, happens.

CISOs can’t be technical peanut butter spreaders anymore. Talk with department/division heads to establish priorities, systems’ value and tolerable downtime. Discuss recovery time objectives (RTOs) and recovery point objectives (RPOs).

Business Interruption Coverage

Business interruption coverage is tricky. From a cybersecurity perspective, it's a challenge to figure out the interruption period. Depending on the source, the average time between the onset of an attack and its discovery can be as much as 270 days – meaning a bad actor has been in place for nearly a year. And, departments or divisions have varying RTOs and RPOs. For a factory line, RTO may be one hour with an RPO of 100%. For finance, RTO may be between now and the next payroll with an RPO of 100%. What is the correct rollback period? Will 30 days suffice? 100 days? Or is the bad actor still present? You can't go back 270 days because the data probably isn't relevant.

From a carrier's point of view, evaluating business interruption is complex, especially when monthly or seasonal revenue fluctuations are involved. Carriers proceed with extra caution. They'll ask if your organization has business continuity and disaster recovery plans, and they may ask for copies or high-level summaries. In some organizations, the lines between these plans are blurred, but they are different. Business continuity planning is based on a thorough business impact analysis of each department's critical applications and processes. Initially, everything is high priority! Keep the conversations going so you can identify the true mission-critical processes and design a plan to address them, considering RTOs and RPOs.

Let's explore a business that makes a majority of its revenue during the holidays. It begins the season with a data security incident that compromises systems. If multiple departments are involved, you need to figure out an absolute recent date to which systems can be restored. If the date is three months ago, what is the true exposure considering the loss of personally identifiable information (PII) and revenue during the busiest time of year? A few weeks earlier or later, the revenue loss would have been substantially less. Carriers find it much easier to underwrite businesses whose revenue is more evenly distributed throughout the year and can restore their systems more quickly.

An additional consideration for business interruption coverage is hidden areas of potentially extreme risk. Both security practitioners and risk managers need to be on the lookout for them and make sure they are included in RTOs and RPOs. These areas might be processes unknown to the security team. Or they might result from legacy customer engagements that involve certain technologies and custom software that operate without security controls. Or they exist in mainframe computers and legacy coding. In the past, bad actors focused on Windows, Linux and Macintosh, so exploring latent areas of risk wasn't of great concern to security practitioners. Now, industrial control systems, micro-controllers and embedded electronic devices (smart thermostats, for example) are targets.

Look for Hidden Areas of Potentially Extreme Risk

An incident that shuts down a chicken processing plant may not be too serious in the long term because workers can process chickens manually. But if the heaters that protect the chicks go down, even for a short time, the chicks die.

Unidentified risk can be disastrous. Blind spots can lead to substantial exposure if they're not found and addressed by security controls and business continuity/ disaster recovery plans.

Another area for scrutiny is third-party applications and APIs. Workloads that are moved to the cloud (someone else's computer) must be included in a risk assessment and insured for business interruption. Insurance carriers are generally up to speed on cloud and will ask:

- Who is your cloud service provider?
- Who are all of your third-party partners?
- What is your architecture – lift and shift or cloud-native, for example?
- How are you protecting cloud workloads?

81% of survey respondents believe that security is the top cloud challenge.[3]

Breach Panels

Enterprises may elect to receive incident response assistance through their insurance carriers or set up a breach panel. Breach panels, also known as data security panels, consist of professional firms that assist in an organization's response to a data incident. Discussions related to breach panels, however lengthy, are beneficial. Pre-approved panel providers and rates can smooth out a policy purchase or renewal. Rates are going up all the time due to inflation and supply-demand dynamics. You never want to be in a position where an incident response provider can demand exorbitant, take-them-or-leave-them rates.

Insurance carriers may dictate approved providers or request that specific providers be added to your panel. Generally, they are open to receiving and giving feedback and will likely be flexible in accepting well-known, reputable vendors. On the other hand, since they are essentially underwriting both your organization and your breach panel, they'll let your risk manager know if they are uncomfortable with a particular vendor based on their evaluation.

Regardless, your risk manager will know upfront the rates that carriers will approve, and your security and riskteams can decide whether or not to cover any difference out of pocket. Every situation is different – but opting to pay the difference may actually save money overall and reduce total damages. For example, it's typically more efficient if a managed security services provider, which is familiar with your organization, can provide incident response, data forensics, recovery assistance and advice to help you prepare for possible future incidents.

Expect to provide the following information to help carriers evaluate your breach panel:

- Bios, hourly rates and background information of providers and their associates, such as public relations or communications firms
- Pre-negotiated terms and retainers
- Secondary, backup providers you've lined up for all firms on the breach panel

[3] Flexera, 2021 State of the Cloud Report

Chapter 4.

Policy Purchase, Non-renewal and Renewal Tips

Many business relationships offer the choice of being a transactional or relational buyer. Be a relational buyer of cyber insurance.

In a dynamic market, it's important to stay the course with your carrier. If you leave, you can't go back. And your organization will carry a black mark for a few years, signaling other carriers to view you as a transactional buyer who will be charged higher premiums. It's tempting to leave after you have a claim and your premium increases, but it's better in the long run to stay put. By paying claims, carriers prove themselves and can reasonably expect your organization to prove itself through loyalty.

> **Cyber hygiene controls are becoming the new minimal standard for companies to secure coverage.[4]**

Be Prepared for an In-depth Examination of Cloud Partners

Insurance companies have access to vast claims data. They know if one of your high-touch partners is a known potential risk. High risk may lead to non-renewal, but you may not know this is the reason.

Use technology that continuously monitors third parties (for reputation, threat intelligence feeds and so on) and scores third-party risk. It's well worth the investment.

[4] Marsh McLennan, The State of the U.S. Cyber Insurance Market

Top Reasons for Non-renewals

Your organization receives a notice of non-renewal. What should you do? Ask your risk manager to speak with the broker and carrier about the reason or reasons and whether they are related to your organization. If you don't have a risk manager, contact your coworker who places insurance. Or, as a last resort, call your broker or carrier yourself.

Sometimes, carriers stop offering cyber insurance, or they reduce limits or just want to initiate discussions that provide information for additional underwriting. Or, carriers may have a negative experience with one or more clients in your industry or with their books of business.

If the non-renewal is about your organization, work with the risk manager to determine if the issue relates to underwriting, the application, technology or something else. However, don't expect many details because neither the broker or carrier want to jeopardize other lines of coverage that are placed or may be placed with your organization. Your risk manager can ask your broker if other clients have received similar non-renewal notices – and ask the following questions to zero in on conditions you can fix:

- Did you scan my system and find something?
- Did you identify something during the underwriting process that indicated a gap or exposure?
- Have underwriting requirements changed specific to our organization? Or the industry?
- Is there something I can do or change to mitigate this non-renewal notice?

Persist in partnering with your risk management department, broker and carrier. Learn what you can about hardening your systems. And push the carriers to provide specific information on non-renewal. If they find a potential issue within your program, other carriers will likely identify it as well.

Preferred Providers

Your carrier will likely have a list of preferred providers – for breach panels as noted above – and also for brands, products and even deployment practices. Rates are lower when you use preferred providers.

Your security team can and should evaluate technology based on requirements, but the next step is to review a carrier's list. If you're on the fence about a provider, go with a pre-approved provider. If you have a claim, the premium won't go up as much as it will if you work with non-preferred providers. And, you can use vetted vendors as a negotiation tactic during the renewal process as well as to improve the claims process.

The Cyber Catalyst by Marsh® Program

Marsh brings together global insurers to evaluate over 90 cybersecurity products and solutions. Reduction of risk is one of six evaluation criteria. Most recently, the insurers targeted products and solutions in these top five categories:

- Ransomware
- Supply chain/vendor management
- Cloud migration and management
- Social engineering
- Privacy regulation/data collection

Source: https://www.marsh.com/us/services/cyber-risk/products/cyber-catalyst.html

Underwriting Evaluation

In the past, carriers used to hire companies like NetDiligence to ask questions on behalf of their underwriters. Now carriers have experts on staff and are more deeply involved in the evaluation/underwriting process prior to approving either an initial policy or a renewal policy. Be prepared to answer questions such as:

- Can we walk through your data center and meet employees?
- Can we set up a conversation with your cloud service provider?
- Can we tag along, virtually or in person, when you tour your cloud service provider's operation?
- What does your cloud infrastructure look like, and how did you move workloads and applications?
- How many cloud hubs are you accessing and are they regional or centralized in one area?
- How frequently are locations creating RTOs and RPOs (flashback to business continuity and business disaster plans)?
- Will you provide screenshots of security configurations?
- If you colocate part of your infrastructure, who is your provider, where is the facility, what does it look like and how does it operate?

Takeaways for colocation? Be transparent with your insurance broker and carrier. Before you make a major decision like colocation that can be difficult to walk back, discuss selection criteria with your broker. A small neighborhood facility may be fine but be sure your broker knows all the details.

If you own your data center, the broker can provide guidance about things that carriers care about – life safety issues, for example. Fire suppression systems can suck oxygen out of the room. Electrical and electromagnetic perils exist. Overhead kitchens, restrooms or restaurants can leak and present water hazards.

Document, Document, Document

Be prepared when you talk to insurance brokers and business continuity and disaster recovery providers. Maintain architectural diagrams of what's in the cloud versus not in the cloud. Where are operating systems, software, code? What parts of your infrastructure are in a colocation data center and what are the facility's physical security controls, certifications, environmental standards and support services? Location changes risk.

Chapter 4. Policy Purchase, Non-renewal and Renewal Tips

Purchase and Renewal Timelines

Collaborate with your risk manager to prepare an initial purchase or renewal application and participate in coverage discussions. Allow plenty of time. Avoid dates that fall into busy holiday periods, ends of months and high-activity months. Insurance binders are typically issued close to the proposed date of coverage or renewal date because carriers want to make sure nothing changes in your organization, claim status or risk exposure.

PURCHASE TIMELINE – APPROXIMATELY 12 MONTHS

Request a full assessment by the broker, who is an advisor and conduit for everything to and from carriers. Assessment fees are typically applied to coverage when placed. Top assessment focus areas include:

- Security protocols and policies
- Information security staff experience and expertise
- Vendors and vendor management process
- Business continuity/disaster recovery processes
- Regulatory and legal compliance for areas such as privacy
- Build a list of what carriers will look for – first 10, next 10 and so on – flagged as must-have and nice-to-have if possible
- Discuss with your broker: security controls, vendors, relationships, provider rates and gaps
- Develop estimates for premiums and incident response scenarios, considering variances in geographic locations

RENEWAL TIMELINE – APPROXIMATELY 6 MONTHS

Start gathering information six months in advance of renewal date:

- A business update, which can include topics such as prior year financials, strategic initiatives and changes in senior leadership and/or geographic markets
- Changes and/or improvements in security controls
- Personnel changes
- Updates on initial assessment focus areas
- Submit the application and supporting documentation to the broker two to three months prior to the renewal date
- Discuss everything with your broker: application details, carrier requirements, potential premium changes (inflation and supply chain issues are factors), breach panel provider rates and so on
- Be prepared to work with your broker to identify and negotiate the major renewal focus – retention, limits, sublimits, waiting periods and so on

Chapter 5. CISO Recommendations

What can CISOs do to help prevent bad insurance events?

Our top 10 best-practice recommendations are:

01 Prepare for rigorous vetting by insurance carriers that will examine credentials, experience and security team bench strength.

02 Have the hard conversations with each department about worth of data (not all data is equal in value) and RTO/RPO.

03 Understand what board members want to hear and know. Research relevant technology and prepare presentation materials that facilitate conversations and decision-making without being too technical.

04 Communicate with and educate board members with complete transparency so they can fulfill their fiduciary duty. Speak their language, verbally and in presentation materials.

05 Practice superior data classification and precise, adaptable protection strategies. Prioritize assets, starting with those most at risk.

06 Build a relationship with the risk manager to eliminate silos and bring technology controls a nd probability of successful attacks into discussions. The more aligned you are with the risk manager, the better you both can perform your primary responsibility in protecting the critical assets of the company.

07 Develop scenarios and worst-case situations with the risk manager to figure out coverage limits. Your company may not be able to purchase insurance for the worst-case scenario. If this isn't possible or feasible, how will the delta be covered and who else needs to be engaged to discuss the probability?

08 Be vigilant about uncovering hidden areas of extreme risk and/or blind spots that carry significant latent risk.

09 Scrutinize third-party relationships from a cyber insurance point of view. Delve into cloud service providers' shared responsibility models to understand what they protect and what your company must protect.

10 Develop a relationship with an incident readiness/incident response provider and negotiate a retainer and rates before an event occurs. Be prepared if you're asked to explain the costs to your insurance broker and why they should be covered by cyber insurance.

Conclusion

Cyber insurance is complicated. Fortunately, CISOs can take steps to reduce complexity and contribute to the cause of getting cyber insurance coverage as right as possible. Your efforts will help educate decision makers, including board members, and propel cybersecurity maturity into the spotlight, where it belongs.

Bring threat intelligence, security control expertise and probability thinking into cyber insurance discussions with your risk manager. Look for opportunities to educate board members and other decision makers about cybersecurity maturity and critical business protections such as business continuity and disaster recovery plans. Explain the importance of continuous security improvement to favorable cyber insurance coverage and rates.

Above all, be unrelenting about vulnerability and risk management throughout your organization to avoid security surprises.

Let's be realistic. The cyber insurance market is known for its ambiguity and obscurity, but it's maturing. Brokers and carriers are clearer about how to balance their risk and your cybersecurity program and controls. Collaboration is the way forward.

To learn more about cyber insurance, view this webinar.

To schedule a conversation or a risk assessment, please contact us.

Cyber Insurance Terms

Actual limits[1] - the most that will be paid by the insurer in the event of a covered loss under an insurance policy, expressed either on a per occurrence basis (e.g., per accident or event) or on an aggregate basis (e.g., all losses under a single policy, or for all policies during an underwriting period).

Sublimit[1] - a limitation in an insurance policy on the amount of coverage available to cover a specific type of loss. A sublimit is part of, rather than in addition to, the limit that would otherwise apply to the loss. In other words, it places a maximum on the amount available to pay that type of loss, rather than providing additional coverage for that type of loss. Example: $10M actual limits, but sublimit of $2.5M for security liability, $2.5M data security incident, $1M for business interruption for any non-IT provider, etc.

Retention[1] - assumption of risk of loss by means of noninsurance, self-insurance, or deductibles. Retention can be intentional or, when exposures are not identified, unintentional.

Exclusion[1] - a provision of an insurance policy or bond referring to hazards, perils, circumstances or property not covered by the policy. Exclusions are usually contained in the coverage form or causes of loss form used to construct the insurance policy. Example: bodily injury or property damage (except not emotional distress), physical event, robocalls, act, error or omission prior to the inception/retroactive/continuity date of the policy.

Endorsement[1] - an insurance policy form that either changes or adds to the provisions included in one or more other forms used to construct the policy, such as the declarations page or the coverage form. Insurance policy endorsements may serve any number of functions, including broadening the scope of coverage, limiting or restricting the scope of coverage, clarifying the application of coverage to some unique loss exposure, adding other parties as insureds, or adding locations to the policy. Endorsements often effect these changes by modifying the existing insuring agreement, policy definitions, exclusions, or conditions in the coverage form or adding additional information, such as insured locations, to the declarations page.

Rate per Million[1] – a unit of cost that is multiplied by an exposure base to determine an insurance premium. An insurance rate is the amount of money necessary to cover losses, cover expenses and provide a profit to the insurer for a single unit of exposure. Rates, as contrasted with loss costs, include provision for the insurer's profit and expenses.

Waiting Period Deductible[1] – a deductible provision sometimes used in business interruption (BI) and other time element policies, in lieu of a dollar amount deductible, that establishes that the insurer is not responsible for loss suffered during a specified period (such as 24 hours) immediately following a direct damage loss.

Cyber Insurance Terms Cont.

Business Interruption[2] – coverage within a cyber policy intended to cover the income loss after a business is impacted by a privacy or security breach; the difference between the typical income of the business and the reduced generated income during the shutdown caused by a cyber event. Business interruption insurance is not included in all cyber policies.

Data Security Panel[1] – a group of professional firms to assist in an organization's response to a data incident. These firms typically include IT forensics and security, PR/communications, defense liability counsel and notification/credit monitoring.

Duty To Defend[1] – a term used to describe an insurer's obligation to provide an insured with defense to claims made under a liability insurance policy. As a general rule, an insured need only establish that there is potential for coverage under a policy to give rise to the insurer's duty to defend.

Duty To Pay[1] – a term used to describe the nature of an insurer's defense obligations under policies. Forms containing duty to pay (or non-duty to defend) provisions require only that the insurer reimburse the insured for funds expended by the insured in defending a claim. In contrast, policies containing "duty to defend" provisions require the insurer to assume control of the claim defense process, including selecting counsel and paying legal bills.

[1] As defined by the International Risk Management Institute (IRMI)
[2] As defined by the Insurance Training Center (ITC)

nuspire | 221b CONSULTING

About Nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @Nuspire

nuspire.com

LinkedIn @Nuspire

Twitter @NuspireNetworks

About 221b Consulting

For more information, visit 221bconsulting.com

221bconsulting.com