WOODRUFF SAWYER

GUIDE TO CYBER LIABILITY INSURANCE

GET STARTED

Cyber Liability Insurance: A Buying Guide

On an almost daily basis, cyber threats of increasing variety hit every size of organization, from small businesses to the federal government. Those who aren't thinking about cyber threats and how to address them may be forced to handle a problem when they least expect it.

This *Buying Guide for Cyber Liability Insurance* will provide the information you need to better identify the cyber risks in your own organization, understand what cyber insurance covers, and recognize how a comprehensive approach is the best way to protect your organization.

8 Reasons to Buy Cyber Insurance

READ MORE >

Getting Started: Cyber Risk Assessment

Identify Common Cyber Exposures | Conduct Cyber Loss Modeling
Assess Your Cyber Security

READ MORE >

Risk Transfer: What's in a Good Cyber Policy?

Key Elements of a Policy | Choosing Limits

READ MORE >

Incident Response: Planning for the Worst-Case Scenario

Incident Response Roadmap | Pre-loss Vendor Onboarding | Claim Advocates

READ MORE >

Cyber Ransomware Scenario

READ MORE >

8 Reasons to Buy Cyber Liability Insurance

1. You're reliant on technology to operate your business.

As organizations increase their use of technology in order to operate, this reliance creates cyber risk. If the technology were to become unavailable, the resulting business impact could be mitigated with cyber insurance.

2. You need to comply with regulations.

There is a wave of consumer privacy rights regulations sweeping the globe, including GDPR in Europe and CCPA in California. Highly regulated industries such as healthcare and finance are no longer the only industries facing the risk of penalties for cyber security and privacy compliance failures. Cyber insurance covers regulatory fines and penalties.

3. Your organization holds a large volume of personal data.

Collecting, processing, and storing large volumes of personal data on customers or employees subjects many companies to state-specific data breach laws. Cyber insurance can help cover costs to comply with state, federal, and international laws.

4. It's part of your board of directors' due diligence.

Many boards have taken a keen interest in cyber security as part of their company oversight role. Cyber insurance is top-of-mind for a diligent board.

5. It's protection when cyber security fails.

Every CISO will tell you that network security is important, but none will say that their security is impenetrable. When security fails, cyber insurance is an important backstop to have.

6. It's a contractual requirement.

Many contracts with vendors or clients require cyber insurance to be in place prior to executing the contract.

7. It comes with a turnkey incident response plan.

Cyber insurance policies come with a team of vendors that specialize in incident response, including legal counseling, IT forensics, consumer notification, on-demand call centers, and public relations specialists.

8. Pre-loss services are included as part of insurance.

Many cyber insurance policies come with pre-loss risk mitigation services included in the premium or offered at a discount. These security tools and best practices can offset security spend and provide significant value, particularly for small-to-medium enterprises.

VIEW LIST OF TOPICS

Getting Started: Cyber Risk Assessment

The first thing you should do when purchasing cyber insurance is conduct a risk assessment, which is a three-step process. In order to effectively transfer risk, it is imperative to identify, quantify, and understand the risks you face as best as possible.

1 STEP 1: Identify Common Cyber Exposures

Cyber risk can take many forms in a modern organization, and trying to comprehend the various ways your company is subject to cyber risk can be a daunting task. Here are four common cyber exposures that impact most companies:

Operational risk lies in a reliance on technology. This dependence on technology for providing services and generating revenue creates a risk to the business in the event of a hack or disruption. If, for example, a certain mission-critical technology is not available when needed, or access to your network is impaired, you may face financial losses due to the interruption of your business activities.

Privacy risk is related to regulations and contractual indemnities that surround the privacy rights of your consumers or other entities with whom you contract. Privacy legislation now defines consumer rights with regard to the collection, processing, storage, and use of data through laws such as the **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act of 2018 (CCPA)**. Additionally, more companies are implementing contractual controls to protect their interests with regard to privacy. Many business-to-business contracts now require indemnification for the damages associated with a data breach.

Security risk is as the name suggests: the risk of a security incident causing damage to an organization. The risk most commonly associated with cyber risk, this can take the form of a data breach, a successful phishing attempt, or a malware attack. The impact from a security incident can be felt both monetarily and reputationally.

Service risk is the failure of your product or service to perform as intended; when viewed from a cyber risk perspective, service risk can be catastrophic to any company. When a cyber attack prevents you from offering your service, it typically doesn't impact just one client but rather all your clients at the same time. This aggregation of risk is the new lens from which companies should understand their cyber risk.

You Can Outsource a Service, but Not Cyber Risk >>

Most businesses today have outsourced services and handed over their data to third parties in some capacity, but they can't outsource their cyber risk.

VIEW LIST OF TOPICS

Assessing Cyber/E&O Risk

Service Risk

Errors & Omissions

- Failure of service or products to perform as intended

Contractual Liabilities

- Indemnification
- Liability caps

Aggregation of Cyber Risk

- Cyber event leading to financial loss for multiple customers at same time

Security Risk

Network Vulnerabilities

- Malware
- Ransomware

Data Breach Risk

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Payment Card Information (PCI)

Confidential Corporate Information

- Third-party confidential information

Privacy Risk

Consumer Privacy Rights

- Data collection, processing, storage, and use

Regulatory Risk

- General Data Protection Requirement (GDPR)
- California Consumer Privacy Act of 2018 (CCPA)

Operational Risk

Reliance on Technology to Operate

- Increase in automation of manufacturing sector
- Increase of cloud adoption
- Enterprise Resource Planning software, such as billing and scheduling

2

STEP 2:
Conduct Cyber Loss Modeling

Once you've identified the primary cyber risks facing your organization, quantify the risk through cyber loss modeling. This process can be used to determine how much risk you're willing to take as an organization and how much risk you'd rather transfer to a cyber insurer.

As with any modeling exercise, the quality and quantity of data will ultimately ensure the accuracy of the modeled results. Modern cyber loss modeling tools illuminate the severity of your potential financial losses under several different scenarios, including a data breach, a network outage, and a software impairment.

Modeling Your Exposures on a Curve

These cyber loss modeling tools simulate a year of potential losses using calculated variables specific to your business, factoring in items such as your size, industry, and PII record count volumes. Sophisticated models don't just calculate an expected loss once, but 50,000 times, in order to provide a customized and comprehensive look at your potential losses on a curve.

The beauty of taking this approach to your customized risk is that most loss scenarios a company would face in a given year can be accounted for on the loss curve. Want to insure against 90% of your projected potential data breach losses? You can find

VIEW LIST OF TOPICS

that on the loss curve to know the proper cyber insurance limit to purchase. Think the most severe losses could never happen to your company? Simply decide to purchase insurance at a lower percentage of the estimated loss.

Modeling Specific Scenarios

Cyber analytics have come a really long way over the past few years. While it's true that using new tools can provide more insights into your overall cyber risk, there are some older models that can still provide useful data for decisions on cyber insurance related to very specific scenarios.

Using data breach calculators, you can model individual scenarios to determine potential losses. These calculators are often a simple math equation based on the number of records exposed, the type of record exposed, and some average values of specific loss types, such as consumer notification costs or credit monitoring costs.

These can be useful in modeling out a single, specific scenario that you'd like to make sure is covered by your insurance. The specific scenario can often get quite granular.

Likewise, business interruption worksheets can give you an estimate of the organization's potential losses suffered during a network outage. A business interruption model can identify insurable losses, such as lost profits and continuing operating expenses, which may be suffered during outages of varying lengths.

As with a data breach calculator, the specific scenarios modeled can be quite granular. A model may display multiple length outages, or sometimes outages at various manufacturing plants individually, to show the effect of a cyber incident at one location or network over another.

Of course, by using a highly specific scenario and only modeling it once, you lose the potential insights into the variance of the loss that a more robust risk modeling tool can provide.

VIEW LIST OF TOPICS

3

STEP 3:
Assess Your Cyber Security

Understanding your cyber security capabilities provides a solid foundation for mitigating the risks you face. In order to assess your cyber security, we recommend first selecting the appropriate framework on which to base your assessment. Several industry groups offer sample frameworks and are good resources to help determine where your security approach needs improvement.

- **NIST (National Institute of Standards and Technology)** maintains a cyber security framework that can help you see where you stack up and is now available to any company.
- **The Center for Internet Security (CIS) Top 20 Controls is** a prioritized set of actions categorized into basic, foundational, and organizational controls.
- **The C2M2 Program is** designed to help organizations improve their cyber security resiliency through a voluntary evaluation process.

Utilizing these frameworks has additional benefits, such as creating a **common language for engaging your board**. Several third-party organizations provide assessments against these frameworks as well.

Cyber Security Controls:
Now Critical for Your Cyber Insurance Renewal >>

Implement a cyber security control, or you might not be able to get cyber insurance at all.

VIEW LIST OF TOPICS

Risk Transfer: What's in a Good Cyber Policy?

Key Elements of a Policy

Cyber liability insurance coverage is generally some combination of **five components**: network security, privacy liability, network business interruption, media liability, and errors and omissions. Network security and privacy liability can include both first-party and third-party costs. Let's go into each element and what it covers.

Network Security

This is coverage in the event of security failure, which can include a data breach, cyber extortion, ransomware, and data restoration coverage. Network security includes first-party costs (i.e., expenses that you incur directly as a result of the cyber incident), which typically include legal expenses, IT forensics, breach notification to consumers, setting up a call center, public relations expertise, or negotiation and payment of a ransom demand. This coverage grant is important for most companies, especially those subject to data risk and privacy risk.

Privacy Liability

Here we have coverage for liabilities arising out of a cyber incident or privacy law violations. These third-party costs can arise from contractual liabilities or regulatory investigations.

Contractual liabilities include any indemnification a company would make with clients to compensate them in the event of a cyber incident or data breach. This policy section also provides coverage for the legal expenses and fines or penalties incurred due to a regulatory investigation. Say a federal or foreign governmental body investigates and levies a penalty for a privacy event or violation—think regulations such as GDPR, CCPA, or FTC privacy consent decrees and their respective fines or penalties. Again, this coverage is important for most companies, particularly those with data risk or privacy risk.

Network Business Interruption

A reliance on technology to operate increases risk for most organizations, but there are options to transfer this operational risk to an insurance carrier through a dedicated cyber insurance policy.

Typically, a cyber business interruption insurance agreement will respond to an operational risk event, allowing you to recover lost profits and fixed expenses incurred during the time your business was impacted.

When assessing coverage for cyber business interruption, there are four key components that should be included in your policy. You can think of it like a matrix: two different event types at two different levels.

66% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result.

Source:
Cybereason, 2021

The two event types that must be present in your policy:

Security Failures

System Failures

The two levels at which they need to be covered are an event on your own company network, and an event on a dependent network—the network of a key supplier or vendor providing services to you.

The security failure event coverage is triggered by the failure to secure a computer system or network. This often results in the transmission of malware, denial of service attacks, unauthorized access or use of the network, damage to a digital asset, or the prevention of authorized, legitimate access to the network, among other digital maladies.

The most common security failure event that has recently led to business interruption claims is **ransomware**. In this attack, attackers will encrypt access to your network drives and data, then offer to restore it for a fee, or "ransom."

The system failure event coverage is triggered by an unintentional or unplanned network outage that is not caused by a security failure. This range of potential events is purposely broad. Computer systems and networks tend to fail, even without an attacker targeting that network.

VIEW LIST OF TOPICS

System failures can be the result of a hardware failure, a failed patch or software upgrade, or even a human error event.

Reputational harm is also part of network business interruption and is the continuing profit impact as the result of a cyber event due to brand reputation damage. This is usually limited to a specific time period and includes aversion to a brand following a publicized cyber event.

Media Liability

This provides coverage for intellectual property infringement resulting from the advertising of your services. It often applies to your online advertising only, including social media posts, but a good broker can negotiate coverage of printed advertising as well.

Errors and Omissions

A cyber event could keep you from fulfilling your contractual obligations and delivering services to your customers. E&O coverage addresses allegations of negligence or breach of contract should this occur, and can include legal defense costs or indemnification resulting from a lawsuit or dispute with your customers.

Choosing Limits

When determining limits, some companies look to their neighbor for context. But peer benchmarking is not a good proxy for choosing what cyber insurance limits to buy. Each business presents unique risks, in the way they collect, handle, and store data, their approach to security, and their appetite for risk.

With the help of your broker, focus instead on cyber loss modeling for your business and your own risk appetite.

Buying the Right Limit with Cyber Analytics: One Size Does Not Fit All >>

This cyber insight discusses not only the right questions to ask, but also the detailed analytics process for determining your cyber risk and how to insure it.

Incident Response: Planning for the Worst-Case Scenario

Your firm has suffered a cyber security incident. The clock is now ticking. What do you do? Are you scrambling to get business back online while worrying about making things right for your customers, employees, and shareholders?

As with any emergency situation, it's crucial to have an incident response plan laid out in advance, which will help you not only get back to business faster but potentially avoid lawsuits and regulatory inquiries as well.

Watch Now: Before an Attack, Incident Response, and Cyber Insurance >>

At time of attack, companies are in pure response mode, stressed. So you need to think about this before an attack on the front end.

Make an Incident Response Roadmap

At Woodruff Sawyer, we walk our clients through an Incident Response Roadmap. This tool imagines different scenarios and pulls out the questions you should know the answers to in advance, such as who needs to be involved in a response to an incident and when to escalate problems within the organization.

Conduct Pre-loss Vendor Onboarding

Select and get acquainted with vendors you would want to turn to in the event of a cyber incident. You can start with your broker or with carriers, which can provide a whole suite of vendors at your fingertips. Being familiar with these companies beforehand will bring you back to business much faster in your moment of need.

Have Claim Advocates Ready to Respond

Did you know that the worst cyber incidents often happen at the end of the workday or over the weekend? If you experience a cyber event, you should make two phone calls: one to your insurance carrier, which likely has a 24/7 hotline, and one to your insurance broker. Woodruff Sawyer's Claims Team provides end-to-end claims support. Our experts help you prevent some claims altogether and fiercely advocate for you if a claim does occur.

Nail Your Communications During a Cyber Event >>

Read more for the three things you should consider when you forge your communications strategy as part of your cyber incident response plan.

VIEW LIST OF TOPICS

Cyber Ransomware Scenario

On Christmas Eve, a Woodruff Sawyer client suffered a ransomware attack, which impacted all laptops, telephones, and servers. The attackers demanded over $13,000,000 to restore the network.

Our Solution

- We immediately connected the client with an IT forensics vendor and breach counsel, which advised on the response to the attacker's ransom demands.
- Using their breach response team, this client determined paying the ransom was not in its best interest, and its cyber insurers supported this decision. Instead, the client chose to completely rebuild its data network from backups, which took nearly 10 days to complete at a cost to the business of over $1,000,000.
- The IT forensics vendor provided expertise on removing data network connectivity from the internet to restore data, patch, and back up all affected laptops and servers.
- The incident response plan permitted the client to harden its internal systems and ultimately enabled the business to return to everyday operations.

Takeaways

- In the initial panic after a ransomware event, many companies are unable to comprehend two realities highlighted by this example: (1) restoring from backups can be more cost effective, and (2) ransoms can almost always be negotiated downward by qualified experts.
- A comprehensive cyber insurance policy supported this client by providing them with the necessary qualified experts through the insurance carrier's panel network of incident response providers.
- The cyber insurance policy paid. In this example, the policy paid out expenses associated with the legal fees, IT forensics investigation, restoration of the network from backups, and the lost profits and continued operating expenses during the 10-day network downtime.

Questions or Comments About This Guide?

Contact your Woodruff Sawyer Account Executive or our National Cyber Practice Leader, Dan Burke.

Dan Burke
National Cyber Practice Leader
dburke@woodruffsawyer.com
LinkedIn
415.402.6514

VIEW LIST OF TOPICS

As one of the largest insurance brokerage and consulting firms in the US, Woodruff Sawyer protects the people and assets of more than 4,000 companies. We provide expert counsel and fierce advocacy to protect clients against their most critical risks in property & casualty, management liability, cyber liability, employee benefits, and personal wealth management. An active partner of Assurex Global and International Benefits Network, we provide expertise and customized solutions to insure innovation where clients need it, with headquarters in San Francisco, offices throughout the US, and global reach on six continents.

For more information
Call 844.972.6326 or visit **woodruffsawyer.com**

Find out why clients choose to work with Woodruff Sawyer

Subscribe for Expert Advice and Insights
Sign up to receive expert advice, industry updates and event invitations related to Employee Benefits and/or Business Risks.

- CYBER INSIGHTS
- D&O NOTEBOOK
- M&A INSIGHTS
- P&C INSIGHTS
- WOODRUFF SAWYER EVENTS

WOODRUFF SAWYER

WOODRUFF-SAWYER & CO.
AN ASSUREX GLOBAL & IBN PARTNER
woodruffsawyer.com