



Guide to Cyber Liability Insurance

2024 Edition

woodruffsawyer.com

WOODRUFF-SAWYER & CO.

Insurance Services | Risk Management | Employee Benefits

Cyber Liability Insurance: A Buying Guide

As the world grows more interconnected and organizations expand their digital capabilities, managing the associated risk has become more challenging. Cyber risk has evolved from a technical problem into a broad business risk. Understanding how to quantify, identify, and transfer an organization's unique business risk has become an imperative.

This *Guide to 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

Getting Started: Cyber Risk Assessment

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

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

Key Elements of a Policy | Choosing Limits

Incident Response: Planning for the Worst-Case Scenario

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

Cyber Ransomware Scenario

8 Reasons to Buy Cyber Insurance

1. **Technology is used to operate the business.**

All businesses use accounting systems, management information systems, point of sales systems, or like tools to operate. It is indeed unfathomable to summon the idea of going back to the days where business was done manually. Cyber insurance is designed to mitigate the financial impact to a business should technology fail or be impacted by a cyber attack.

2. **The organization is subject to cyber and/or privacy regulations.**

Organizations must conform to new federal, state, and industry privacy and reporting regulations that require additional policies and consent procedures, enhanced proactive security measures, and the disclosure of security incidents to numerous regulators in a short timeframe. 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. **The organization holds a large volume of personal data.**

The organization is collecting, processing, and storing large volumes of personal data on customers or employees. If there is a breach the organization may have notification requirements to individuals. Cyber insurance can help cover costs to comply with state, federal, and international notification laws as well as the cost of credit monitoring services to those affected.

4. **It's a key objective for the board of directors' due diligence.**

Oversight of the cybersecurity risk is an important part of the board's 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. **You are implementing a new AI technology and are concerned about unforeseen risk.** Some of the risk surrounding AI usage is data leakage or an inadvertent breach. A well placed and crafted cyber policy is an important tool when using a rapidly changing technology.

8. **You are concerned about the impact from third-parties.** Today's organizations don't operate in isolation. Most rely on an intricate array of third-party relationships that extend the physical and virtual boundaries. However, third party can also have an impact to an organization's cyber risk. A well placed policy will contemplate coverage for this risk.

Getting Started: Cyber Risk Assessment

The first step to take in preparing to purchase cyber insurance is to 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.

STEP 1: Identify Common Cyber Exposures

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

Understand and quantify the business impact. Dependence on technology for providing services and generating revenue creates a risk to the business in the event of a cyber incident or network disruption. If, for example, a certain mission-critical technology is not available when needed, or access to the network is impaired, financial losses due to the interruption of your business activities may ensue.

Privacy risk – The complexity, variety and scale will vary from organization to organization, but all organizations that process personal data have privacy risk. Organizations must grapple with an increasingly complex privacy risk environment and evolving regulatory requirements. This is compounded by the introduction of emerging technologies, changing consumer expectations on privacy, and increasing scrutiny on business initiatives and market trends by regulatory bodies.

Security risk is the risk of loss of confidentiality, integrity, or availability of data, information, or systems. 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.

Production or services losses – A cyber attack can create a disruption to the ability of an organization to perform as intended; risk to production or services can be catastrophic to any company. When a cyber attack disrupts operations and production or services are paused, 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.





Digital Supply Chain Risk – Any critical risk posed to your organization from a third party service. These third parties could be integrated suppliers, software services, outsourced technology management etc. Identifying and understanding how these third parties' cyber vulnerabilities could impact your business is crucial to knowing the totality of 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.**

Assessing Cyber/E&O Risk

 Transactional Risk	 Security Risk	 Privacy Risk	 Business Impact
<p>Errors & Omissions</p> <ul style="list-style-type: none"> • Failure of service or products to perform as intended <p>Contractual Liabilities</p> <ul style="list-style-type: none"> • Indemnification • Liability caps <p>Aggregation of Cyber Risk</p> <ul style="list-style-type: none"> • Cyber event leading to financial loss for multiple customers at same time 	<p>Network Vulnerabilities</p> <ul style="list-style-type: none"> • Malware • Ransomware <p>Data Breach Risk</p> <ul style="list-style-type: none"> • Personally Identifiable Information (PII) • Personal Health Information (PHI) • Payment Card Information (PCI) <p>Confidential Corporate Information</p> <ul style="list-style-type: none"> • Third-party confidential information 	<p>Consumer Privacy Rights</p> <ul style="list-style-type: none"> • Data collection, processing, storage, and use <p>Regulatory Risk</p> <ul style="list-style-type: none"> • General Data Protection Requirement (GDPR) • California Consumer Privacy Act of 2018 (CCPA) 	<p>Reliance on Technology to Operate</p> <ul style="list-style-type: none"> • Increase in automation of manufacturing sector • Increase of cloud adoption • Enterprise resource planning software, such as billing and scheduling

**STEP 2:
Model Cyber Losses**

After identifying the cyber risks facing the organization, one can quantify the risk through cyber loss modeling. This process can be used to determine how much risk an organization is willing to retain and how much risk it will 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 Exposures on a Curve

Cyber loss modeling tools simulate a year of potential losses using calculated variables specific to the business, factoring in items such as the 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 the potential losses on a curve.

The advantage of taking this approach to 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 that on the loss curve to know the proper cyber insurance coverage amount or "limit" to purchase. Modeling will help identify the relative exposure to multiple cyber threat scenarios. Simply decide to purchase insurance at a lower percentage of the estimated loss.

Modeling Specific Scenarios

Cyber analytics have come a 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.

STEP 3: Assess Your Cyber Security

Understanding your cyber security capabilities provides a solid foundation for mitigating the risks you face. To assess 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.

Using 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.

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, crisis management and communications, and negotiation and payment of a ransom demand by a seasoned cyber threat actor negotiator. 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.

The two levels at which events 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

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



Security Failures



System Failures

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.

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.



The global annual cost of cybercrime is expected to reach US \$9.5 trillion in 2024 (eSentire). The damage from a cyber attack requires about 277 days to remediate (IBM 2023).



**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 >>

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.

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.



Build a Crisis Communication Strategy >>

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

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 million 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 million.
- 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 about this Guide? Comments? Compliments?

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



Dan Burke
National Cyber Practice Leader

dburke@woodruff Sawyer.com
415.402.6514

As one of the largest independent 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 [woodruff Sawyer.com](https://www.woodruff Sawyer.com)

Additional Resources

Subscribe for Expert Advice and Insights

Sign up to receive expert advice, industry updates and event invitations related to business risks.



Cyber Notebook

Cyber Liability Insurance, Privacy Legislation, Cyber Risk Mitigation



D&O Notebook

D&O Insurance, Corporate Governance, IPOs, Board Issues



P&C Notebook

Property, Casualty, Risk Management, Claims, Workers' Compensation



Events & On-Demand Webinars



**WOODRUFF
SAWYER**

[woodruff Sawyer.com](https://www.woodruff Sawyer.com)

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