GUIDE TO CYBER LIABILITY INSURANCE

GET STARTED
Cyber Liability Insurance: A Buying Guide

New cyber threats emerge nearly daily, hitting every size 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 address a problem when they least expect it.

In this Guide to Cyber Liability Insurance, you will learn to better identify the cyber risks in your own organization, understand what cyber insurance covers, and how a comprehensive approach is the best way to protect your organization.

8 Reasons to Buy Cyber Liability 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 >

How Other Policies are Impacted by Cyber Risk
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. 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 after an incident.

2. You're reliant on technology to operate your business: As organizations increase their use of technology in order to operate, that reliance creates cyber risk. If the technology were to become unavailable, the resulting business impact can be mitigated through cyber insurance.

3. Comply with regulations: Highly regulated industries such as healthcare and finance must be in compliance with data security provisions or face penalties. Cyber insurance covers regulatory fines and penalties.

4. It's a contractual requirement: Many contracts with vendors or clients require cyber insurance to be in place prior to executing the contract.

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 comes with a turn-key incident response plan: Cyber insurance policies come with a team of vendors that specialize in incident response—from legal counseling to IT forensics, consumer notification, on-demand call centers, and public relations specialists.

7. 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 with a diligent board.

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.
Getting Started: Cyber Risk Assessment

In purchasing cyber liability insurance, you should first 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 risk 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 your company is subject to cyber risk can be a daunting task. Here are three common cyber exposures that impact most companies:

Privacy liability is exposure 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 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 regards to privacy. Many business-to-business contracts now require indemnification for the damages associated with a data breach.

Informational risk is data breach risk. Whether that data is personally identifiable information on customers or employees (such as medical information, SSNs, etc.) or sensitive third-party corporate information, the threat of that information getting accessed, lost, stolen, or held for ransom, and the resulting financial fallout, is a risk for many organizations.

### 446.5 Million Records Were Exposed in 2018 Due to Data Breaches

<table>
<thead>
<tr>
<th>Category</th>
<th>Records Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Credit/Financial</td>
<td>1,709,013</td>
</tr>
<tr>
<td>Business</td>
<td>415,233,143</td>
</tr>
<tr>
<td>Education</td>
<td>1,408,670</td>
</tr>
<tr>
<td>Government/Military</td>
<td>18,236,710</td>
</tr>
<tr>
<td>Medical/Healthcare</td>
<td>9,927,798</td>
</tr>
<tr>
<td><strong>Annual Totals</strong></td>
<td><strong>446,515,334</strong></td>
</tr>
</tbody>
</table>

© Woodruff-Sawyer & Co., 2019
Operational risk is 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 technology is not available or your network goes down, you may face financial losses due to the interruption of your business activities. This operational risk can extend to your suppliers as well. As you consider the operational risk of a cyber incident to your own organization, you should also consider the operational impact of a cyber incident at a key supplier or vendor.

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. Use the risks identified in Step One when generating models.

There are multiple ways to calculate cyber loss models:
- Assess aggregated contractual liabilities across your contracts or potential damages associated with regulations, such as GDPR or CCPA.
- Calculate the cost of a data breach.
- Quantify the financial impact of a business interruption event.

These models should be highly customized to the organization. A good broker makes sure that clients are very involved in this part of the process, identifying factors such as seasonality in your business and the specific types of information or data you carry. For example, when looking at the potential impact of a business interruption due to a cyber event, the model is adjusted based on the likelihood of impact to revenue or based on the cost of replacing systems.

The more accurate and detailed information that goes into these calculations, the more accurate the loss models, which will in turn allow you to determine the most appropriate cyber insurance limits to purchase.
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 maturity, we recommend first selecting the appropriate framework from 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 C2M2 Program** — designed to help organizations improve their cyber security resiliency through a voluntary evaluation process.

• **The Center for Internet Security (CIS) Top 20 Controls** — a prioritized set of actions categorized into basic, foundational, and organizational controls.

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.

Woodruff Sawyer has created our own team of recommended experts specifically for this purpose. The **Cyber Services Network (CSN)** is a group of vetted, trusted cyber security experts that we tap into on our clients' behalf, proactively mitigating the risk of cyber attacks.

**Cyber security services that the CSN can provide:**

• Vulnerability testing
• Penetration testing
• Tabletop exercises
• Mergers & acquisition risk assessment
• Incident response readiness assessment
• Board of directors presentation counseling
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 (expenses that you incur directly as a result of the cyber incident). These costs 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, including 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. This coverage is, again, important for most companies, particularly those with data risk or privacy risk.
Network Business Interruption
How dependent is your organization on technology to operate? Network business interruption coverage provides a solution for companies that face an operational cyber risk. When your network, or the network of a provider that you rely on to operate, goes down due to an incident, you can recover lost profits and fixed expenses incurred during the time your business was impacted. This includes loss arising from a security failure, like a third-party hack, or a system failure, such as a failed software patch or human error.

Reputational harm is also part of network business interruption and is the continuing profit impact 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 only to your online advertising, including social media posts, but a good broker can negotiate to have printed advertising covered as well.

Errors and Omissions (E&O)
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—from the way data is collected, handled, and stored, to your approach to security and your appetite for risk.

With the help of your broker, focus instead on cyber loss modeling for your business (see above) and your own risk appetite.
How Other Policies are Impacted by Cyber Risk

Cyber risk takes many forms. So can the insurance policy for a cyber incident. It's important to have a broker explain how other policies you already have respond to cyber incidents—and when they won't. Be aware that just because you have other policies that may be activated in the event of a cyber incident, there are probably gaps around which damages they'll actually pay.

And trying to find coverage for the consequences of a cyber incident on non-cyber policies is a gamble. In fact, there are a number of lawsuits from companies against insurance carriers due to their **cyber claims not being covered by non-cyber policies.**

Here are some examples of how losses can manifest out of a cyber incident and the potential response (or lack thereof) from various insurance policies.

### Will Your Non-Cyber Policies Cover You for a Cyber-Related Incident? Maybe Not.

<table>
<thead>
<tr>
<th>Consequences of Cyber Breaches</th>
<th>Data Breach of PII or Client IP</th>
<th>Loss of Own IP</th>
<th>Network Business Interruption</th>
<th>Theft of Money</th>
<th>Explosion/Property Damage</th>
<th>Bodily Injury</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Insurance Policy Response</td>
<td>Cyber or E&amp;O</td>
<td>Not Covered</td>
<td>Cyber Business Interruption</td>
<td>Crime Policy; Some Cyber Policies</td>
<td>Property and Property Business Interruption</td>
<td>General Liability or Products Liability</td>
</tr>
</tbody>
</table>
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? Would you be 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.

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.

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 insurance 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.

Claim Advocates

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 carrier, which likely has a 24/7 hotline, and one to your 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.
Cyber Ransomware Scenario

One Thursday night, a Woodruff Sawyer client was attacked by ransomware.

63 servers, two laptops, and their entire dataset were encrypted.
The Ransom: ½ bitcoin per server, equaling $200K

Our Solution
We immediately connected the client with an IT forensics vendor, which:

• Advised on response to attacker’s ransom demands

• Provided forensic expertise to restore data, patch, and back up all affected laptops and servers.

• Allowed the client to harden its internal systems and get the business back online starting Friday and more fully by the following Monday.

Takeaways

• Using the Breach Response Team, this client saved half of the expenses they would have incurred from this attack.

• If the client had cyber liability insurance, 90% of this cost would have been recoverable.

• Expenses from the attack were $75K–$100K, not including employees working day and night.

Managing your business risk in an ever-evolving digital world can be difficult and time consuming, but insuring your liability is imperative to your company’s security and success.

Questions or Comments About This Guide?
Contact your Woodruff Sawyer representative or our National Cyber Practice Leader, Dan Burke.

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

- WOODRUFF SAWYER WEBSITE
- D&O NOTEBOOK
- CYBER INSIGHTS
- M&A INSIGHTS
- P&C INSIGHTS
- DATABOX: FOCUS ON D&O LIMITS
- WS SEMINARS & WEBINARS