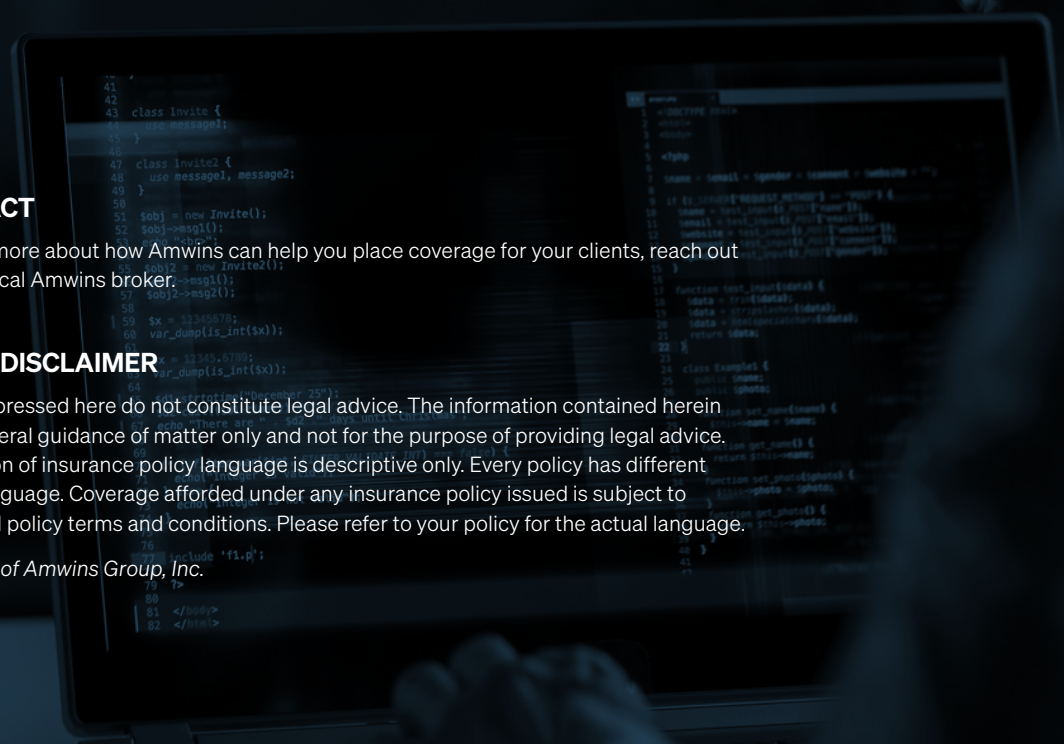
AMWINS

Navigating Cyber Insurance for Vendor Agreements

When you combine the potential for **more than 3,000 data breaches** every day with an expected increase of nearly 10% each year in the **global business process outsourcing market**, it's easy to see why the need for cyber liability insurance is expanding.

Every business is at risk for a cyberattack – either directly or indirectly. While a business may not rely on a sophisticated computer network or process confidential information, odds are the business is dependent on other entities who operate networks and process data that belongs to the business. And with data breaches costing an **average of $4.88M per incident** in 2024, the best defense may just be a good offense, which comes in the form of carefully written contracts and insurance policies.



CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

07.25

Should a vendor be required to carry a cyberliability policy?

Asking vendors and third parties to carry a cyberliability policy can help provide coverage for losses related but not limited to data breaches, ransomware attacks, phishing, social engineering, dependent business interruption, etc. However, a vendor's traditional "off the shelf" cyberliability policy may not address any downstream risk or potential loss for your client.

Work with your client to help ensure that the vendor's policy:

- Names the client as an additional insured
- Includes a waiver of subrogation provision
- Is considered primary and not contributory
- Remains in place for as long as services/products are provided, plus a minimum of five years after the contract ends

You may also want to require that the vendor not cancel or modify their policy without your client's consent.

What if the vendor has access to PHI and/or PII?

It's important to understand what information the vendor will be processing. Will they be handling census information, demographics, Social Security Numbers? Is there health information and will any of that information fall outside of HIPAA? Defining this within the policy can help eliminate confusion.

PHI (protected health information): A **BAA (business associate agreement)** outlines the requirements and prohibitions for protecting PHI when disclosed. These agreements are required by the **HITECH Act of 2009**. Be sure to include how a disclosure is identified, as well as specific technical controls required to protect the PHI. Understanding what the vendor is technically able to accommodate will be key to averting coverage that meets only the minimum requirement.

PII (personally identifiable information): Without a federal privacy law in the U.S., jurisdictions have developed their own definition of PII. For example, a vendor located in Virginia may do business with companies in Texas, California and Colorado. Each state likely has different privacy laws that may impact the vendor's coverage. So, having a contract in place that provides comprehensive coverage means the insured will need to acquire more than the bare minimum of coverage required for any one jurisdiction.

Is there anything else to watch out for?

If the vendor is providing professional services/products to your client that involve the handling of private information, you may also want to ensure that:

- Coverage limits are the same for both E&O and cyber (e.g., if E&O is $5M then cyber should be $5M).
- Coverage for both E&O and cyber is included in a single policy. A combined policy can help address situations such as an allegation of an error in providing a professional service, as well as a privacy or security breach.
  - If separate policies must be purchased, confirm there are no significant exclusions in the cyber form that eliminate or narrow coverage. Purchasing either E&O or cyber coverage alone can result in a dispute over allocation of coverage from covered and uncovered matters.
  - If separate policies are purchased from different insurers, conflict can arise between insurers over which expenses are covered by the policy they issued.

You'll also want to consider maximum retention provisions as well as notification requirements that require indemnification from vendors for first-party costs.

Are business interruption and/or data recovery expenses covered?

After first determining that the vendor has a cyberliability policy, the next step is to establish exactly what the policy covers and clarify the vendor's liability. If the vendor experiences a data breach or ransomware attack, will the policy cover your client's resulting losses?

Policy coverage limits typically depend on the size of the vendor and the type of services/products they provide. You will need to help determine if the vendor's coverage is enough to make your client whole if they can't do business because of a data breach or cyberattack. If not, is your client prepared to make up any difference or will they require the vendor to increase coverage?

Remember, even if the vendor doesn't handle data for your client, that vendor likely relies on various systems to keep them running. Help your client ensure that they are covered in the event the vendor's systems go down and the supply chain is negatively impacted.

How can coverage gaps be identified?

While every insured is different, there are some things to watch out for:

- **Does the vendor carry cyber insurance?** If not, work with your client to request the vendor carry coverage in an amount deemed necessary for the type of risk they are assuming.
- **Does the vendor's insurance help cover your client's losses** in the event of a data breach or does it simply help the vendor keep their doors open for business? Has your client been named as an additional insured?
- **What types of services/products are covered?** Is there a limitation of liability or a cap on damages?
- **Is the vendor's policy in compliance with contract provisions?** Be sure to verify that the vendor meets data encryption requirements, has the appropriate data backup procedures in place and agrees to follow all regulatory compliance.

It's also imperative that any and all exclusions are thoroughly vetted and understood so that no gaps in coverage remain.

Should subcontractors be required to carry additional coverage?

Vendors handling PHI or PII will typically ask a subcontractor to agree to terms that are no less favorable or restrictive than what their own policy covers. There may be slight differences in their contract for services, but in general this is a practical consideration and one the subcontractor should not have a problem agreeing to. In a worst-case scenario, your client can require proof of insurance of all vendors and subcontractors.

What if the client – not the vendor – is responsible for the breach?

Up to this point, we've focused on data breaches and attacks on a vendor's system. But what if it's your client that has the breach? Your client should have a cyberliability policy that covers their own expenses related to breaches. As an additional layer of risk mitigation beyond the contractual transfer of risk, your client's cyberliability policy will also likely cover losses caused by vendor breaches.

Regardless of the industry, every business is at risk for a cyber-attack. So, while certain industries are more vulnerable than others, a proactive strategy is often the most effective form of protection. Having the proper cyber security controls in place, such as multi-factor authentication and end point encryption, combined with a cyber policy can help protect your client from cyber risks as they emerge. It's better to avoid a breach altogether to avoid indemnity fights between clients and vendors.

Which insurance policy responds first?

Let's assume the business and its trading partners have purchased cyber liability insurance as well as additional insurance policies to protect each other from any potential problems arising from the trading relationship. Each entity has strong contracts that shift liability and address additional insureds where applicable, and both parties are comfortable with the limits and coverage terms.

However, there's a catch. Cyberliability policies are designed to cover a business's own expenses arising from a cyber event wherein the breach occurs on their system. This could include forensic, data recovery, legal and business interruption expenses; ransom payments, regulatory fines and penalties; as well as liabilities the company incurs in the event it is sued by its trading partners. This is commonly called "first party cyber coverage."

If there is a financial loss caused by a cyber event occurring within the vendor's or client's system, will their policy step in to cover the company's losses or will the company have to sue the vendor and win to collect under the vendor's policy?

This is an important consideration since it is likely that from the moment the vendor becomes aware they have a problem, they'll be focused on researching and stopping the threat for their own benefit. Their clients' interests will be secondary. You will need to work with your client to determine if it is their expectation that the vendor's insurance will make them whole, or if their own policy will protect their interests.

The devil is in the details. We see many contractual demands for vendors to purchase cyber liability insurance, but very rarely does the requirement address how the vendor's insurance will actually address the company's interests.

This is where the insured, insurance brokers and underwriters need to have an open dialog about the coverage working as intended. The last thing anyone needs after a meaningful cyber event is a conflict between trading partners.

Takeaway

From small businesses to Fortune 500 companies, Amwins partners with you to find the right coverage for your clients — no matter their size or complexity. We stay on top of emerging cyber threats to develop new products that protect your clients from cyber risks as they emerge and offer our clients **discounts with industry-leading cyber security service providers** to help insureds improve their risk profile.

With our cyber liability expertise, resources and insurance products. Amwins is here to **help protect your clients from a web of cyber threats with tailored cyber insurance solutions**.

Insights provided by:

- David Lewison, EVP and Amwins National Professional Lines Practice Leader
- Peter McClelland, Assistant General Counsel, Amwins
- Pamela Mims, Deputy General Counsel, Amwins
- Jamie Orye, EVP, Profinity Insurance Services
- Holly Roberts, Esq., Of Counsel, Amwins