AmWINS Group, Inc.

CLIENT ADVISORY

What is Cyberliability?

The term "cyberliability" is one that has evolved over the past decade. There were policy forms called cyberliability insurance in the past that were written as professional liability policies for companies providing a wide variety of computer hardware and software services. Many of those forms included coverage for the company's own website design, content and services. The somewhat vague term "cyberliability" has stuck, yet the coverage has grown and is now available for many other industries – not just technology providers.

Often, contractual requirements for cyberliability have no clear description of the scope of coverage necessary. Insurance buyers can approach this in two ways: 1) They can use that lack of specificity as an excuse to buy cheap cyberliability that doesn't fit the exposures contemplated in the contract; or 2) They can purchase a broad cyberliability policy that matches the exposure – if they don't already have the proper type of coverage. You may not know which type of form will make sense without first understanding the different options available.

Traditional cyberliability policy coverage included the following: Third party liability coverage for alleged wrongful acts arising from the performance of services as a technology professional or consultant. Typical covered services included computer hardware/software consulting, system integration, website design, online services and content, and online commerce. The definition of wrongful act may or may not include a personal injury component, which could include an invasion of privacy. The definition of wrongful act may or may not include liability coverage for a breach of security caused by the named insured. There are technology insurance policies in the marketplace that specifically exclude security liability.

Modern definition of cyberliability policy can include some or all of the following:

- The same third party technology professional insurance as above
- Privacy Liability (Covers loss of personally identifiable employee and customer information.)
- Security Liability (Covers failure to prevent the entrance or spread of a virus/hacker attack.)
- Website Media Liability (Covers libel, slander and copyright infringement from your website content.)
- First Party Cyber Extortion (Covers expenses to respond to a threat to harm or release your data as well as cover ransom payments if necessary.)
- First Party Privacy Breach Response (It is common to sublimit the coverage to an amount lower than the annual aggregate limit.)
  - Customer Notification Expense
  - Credit Monitoring Expense
  - Computer and Legal Forensic Expense
  - Credit and Identity Repair Expense
- First Party Business Interruption and Data Recovery Extra Expense
- Regulatory Defense and Penalty

It is important to remember that no two policies are identical and the terminology can often be confusing.

Why did the new type of cyberliability policy come to exist? For many years there has been awareness that companies should be accountable for private records they handle or control. One law that raised awareness was the Health Insurance Portability and Accountability Act (HIPAA) of 1996. In 2003 a privacy rule went into effect for the private healthcare information protected under HIPAA. Since then, 46 out of 50 states have also amended their state laws or codes to also address how companies and state agencies must respond to leaked personally identifiable information (PII). Most state laws say that if you lose records of a state resident, you must notify that state resident so he or she has the ability to take the proper defensive steps as well as notify a specific state agency and/or

To learn more about cyberliability, reach out to your AmWINS contact or send an email message to marketing@amwins.com.

If you do not have a financial services contact at AmWINS, click here for a list of brokers on our website.

AmWINS Group, Inc.

AmWINS Group, Inc. is a leading wholesale distributor of specialty insurance products and services. AmWINS has expertise across a diversified mix of property, casualty and group benefits products. AmWINS also offers value-added services to support some of these products, including product development, underwriting, premium and claims administration and actuarial services. With over 1,800 employees located in 16 countries, AmWINS handles over $5 billion in premium annually through our four divisions: Brokerage, Underwriting, Group Benefits and International.

AmWINS Group, Inc.

CLIENT ADVISORY

What is Cyberliability?

Why did the new type of cyberliability policy come to exist? (cont.)

state attorney general. It does not matter where your company is located; the notification requirement is dictated by where the victim currently resides. Though not explicitly defined, your responsibility to keep records private is not eliminated when one of your vendors holds PII on your behalf. If it is your customer, you remain responsible for the security of the data. Notification of the individuals can get complicated as people are known to move from state to state and many businesses transact across state lines. To look up the state laws, please check the following website: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

The privacy laws referenced in the paragraph above apply to all types of business, not just technology businesses. If we only offered the traditional cyberliability policies, then only technology companies providing technology services would be able to find coverage. Since the exposure exists for any type of organization that handles private information, a new type of policy had to be created. This coverage is also not limited to electronic records. Most current cyberliability policies (also known as security and privacy policies) cover personal records in any format including paper records. As mentioned earlier, all organizations with PII have exposure. Businesses such as health care providers, law firms, accountants, hotels, retail stores, schools, public entities, charitable organizations, mortgage brokers, insurance agents and restaurants all have the exposure.

As this exposure has evolved, so have the policy forms. Around 2003 when the privacy rule under HIPAA went into effect, there were a handful of policies available that could provide some assistance in the event of a data breach. Now there are more than 30 dedicated policy forms. Easily half of those forms have been created and released in the past 18 months.

Please contact your AmWINS Financial Services broker to assist you in determining which policy form is the most appropriate for your client.

PRIVACY & SECURITY QUICK REFERENCE GUIDE

Third Party Liability Coverage	
Security	Failure of network and information security to prevent the transmission of computer viruses or the penetration of a hacker.
Privacy	Failure to protect private or confidential information.
Media/Content	Libel, slander, and other forms of disparagement, etc. with respect to display of material online as well as infringement of a copyright by your website content.
Regulatory Actions	Regulatory actions brought by state or federal agencies to enforce privacy regulations.
First Party Coverage	
Business Interruption	Interruptions in business due to breaches of a company's network (e.g. denial of service attack).
Crisis Management	Expense of retaining a public relations firm to help mitigate damage to the insured's reputation and brand image (typically sub-limited).
Extortion/Threat Expenses	Costs to investigate, negotiate and settle threats made against the insured related to intentional computer attacks.
Privacy	Expenses for breach response services such as notification, credit monitoring and identity/credit repair.