10 Things to Ask When Purchasing a Cyber Crime Policy

January 22, 2019

If title or settlement company has decided to obtain a cybercrime policy, here are 10 questions from the Title Industry Assurance Company to help guide you through the process and find the right policy based on your company's needs and vulnerabilities.

What type of cybercrime is my company most vulnerable to?

Evaluating where you believe you're most likely vulnerable will help to understand the coverage(s) you truly need. Cyber fraud/social engineering, data breach, extortion and network intrusion are the most common exposures to consider for coverage.

Who should carry cyber liability coverage?

If your company handles any personally identifiable information for your customers or employees, you should have a cyber liability policy. Also, if you provide financial transactions, your company should have a cyber liability policy in place.

What are my coverage options? What does a policy cover?

Contemplating the type of exposures you are most vulnerable to is where you need to start your evaluation. You then need to decide what coverage options are most critical to your business. Is it cyber deception or email fraud? Is it public relations to manage your reputation should a breach occur? Is it the cost of notifying clients? Regulatory fines? Investigations? Determining what is important will help you have a discussion with an insurance professional to figure out he right coverage.

Third-party Coverage: Does the policy provide coverage for companies used by you?

Most companies use third-party providers/vendors to manage or store data or to perform business functions. If you experience a breach or cybercrime as a result of a third party are you covered or does the third-party vendor have coverage in place that will also protect you?

Third-party coverage for social engineering/cyber deception coverage: Does my policy provide coverage?

For the title industry, this is the most vulnerable exposure. You'll want to have a discussion with your insurance professional to ensure the policy you are purchasing or currently have provides this coverage. Third-party exposure in this realm involves cases when a hacker causes someone in a real estate transaction to wire funds to a fraudulent account. This action may not have been a result of any wrongdoing on your part, but you

are brought into a claim because of the services you provided in the transaction. You must ensure the language in the policy defines social engineering or cybercrime/ cyber deception AND provides third-party coverage.

If my policy provides coverage for social engineering/cyber deception is there an authentication clause or "call back" clause?

More carriers are providing social engineering coverage for their policies to be relevant and time sensitive. However, many are adding the further requirement that you must confirm that contact was made to authenticate the validity of an email regarding wiring instructions. This authentication must be made by telephone call and via email. If such contact isn't made, a claim for coverage would be denied. It's important to know about this type of requirement before purchasing a policy.

Is my coverage retroactive?

Coverage usually initiates after an attack has already occurred, and many policies don't cover any expenses prior to this date. That means, if you've already lost thousands of dollars from a denial of service attack before reporting it to your insurance company, you won't be able to obtain coverage for those losses. If you're concerned about undiscovered cyber incidents that may have occurred in the past, be sure to negotiate an appropriate retroactive date with your policy provider. This is especially helpful if coverage is only triggered after claims are made. Most carriers can provide full prior acts coverage from the inception date of the policy.

Does the policy include credit and identity theft monitoring?

Fraud through identity theft is a common occurrence for companies. Check to see if this is included in your policy and exactly who will be covered by it.

What crimes are potentially not covered?

Once you have had an opportunity to review coverages and polices with your insurance agent, consider not only the crimes the policy will cover, but what potentially isn't covered. Discuss these risks with your internal cybersecurity team to ensure you've made the best decision.

Doesn't my professional liability or E&O policy include cyber coverage?

Many companies believe that cyber liability risks are already covered by professional liability insurance. While your policy may provide some coverage for cyber liability risks, there are often huge gaps or grey areas. Also, if you have a breach or hack and need to make a claim against your professional liability policy—it could affect your premium and continued insurability. The best option is to secure a standalone cyber-liability policy.

*Contact ALTA at 202-296-3671 or **communications@alta.org**.*