

Five Things to Consider When Purchasing Cyber Liability Insurance

Description

The FBI's Internet Crime Complaint Center (IC3), which has been monitoring cyber criminal activity since 2016, received a record number of cybercrime-related complaints from the American public in 2020: Nearly 800,000 – a 69-percent year-over-year increase, with reported losses exceeding \$4.1 billion.

As cyber fraud attacks increase in volume and sophistication, many title companies are turning to cyber liability insurance to shield themselves from the harmful effects of business email compromise, theft of wired funds and other types of cybercrime. However, in a NATIC educational webinar, "Cybersecurity Must-Haves and Misconceptions," Alex Kidd, vice president and director of Quality Assurance and Compliance for Lennar Title, shared some words of wisdom for agents who may be considering adding additional protection to insure their clients' funds and manage their risk.

"Cyber liability insurance is obviously something all agents should consider," Kidd said. "Although most underwriters don't require it, I think it's necessary because if you have, say, a \$400,000 loss, you may not be able to cover it, and you'll be out of business."

Cyber insurance coverage options vary greatly and may be offered on a standalone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions or directors' and officers' policies. Cyber coverage options may also be structured as first-party coverage, which insures against direct expenses incurred by the insured party, or third-party coverage, which protects against claims made by financial institutions' customers, partners or vendors.

Kidd listed several important factors to consider if your company is weighing adding this type of insurance coverage.

1. Not all policies are created equal. "Every insurance agent will tell you that, and it's part of their sales pitch to you, but it's true," Kidd said. "It may not cover all thefts involving technology. It does not cover every type of theft. Insurance companies tend to be very broad in their scope of coverage, and some of them are still identifying and labeling the different types of cybercrime."

2. Your crime insurance or errors and omissions policies may already provide you with some level of cyber fraud protection.

"It's quite possible you are covered if theft is involved," Kidd said. "You may have endorsements that cover specific types of occurrences, depending on the type of cybercrime involved or whether it was a hard or soft breach. If someone came in and stole your computer, you probably will be covered in some way by these types of policies."

3. Consult with a professional insurance agent who specializes in business and liability to find out what types of policies are available. "You may have to obtain several endorsements, because that is how they shield themselves from claims," Kidd said. "You need to decide what type of policy is right for

you based on the type of business you are in. For example, if you deal with a lot of commercial transactions, you may face fewer risks because there are a lot of attorneys and third parties involved. If you do most of your business on the retail side or work with affiliated real estate agents, you should gauge exactly what your risks are. That's going to vary for everyone.â•

4. Don't forget your statutory reporting responsibilities. Regardless of the type of insurance policy you obtain, many states have enacted laws around specific transaction value and loss thresholds, Kidd cautioned. He noted that if you are a multistate operator, "you must follow the state's law where the customer is located, not necessarily where you are domiciled or physically located, because states enact laws to protect their citizens.â•

5. Purchasing cyber liability insurance does not remove the need for a sound control environment. Rather, it should be a component of a broader risk management strategy that includes identifying, measuring, mitigating and monitoring cyber risk exposure, Kidd concluded.

VLTA Examiner



Amy Tankersley

Industry & Vendor Relations Manager
North American Title Insurance Company (NATIC)

Category

1. Cybersecurity

Date Created

2021/12/22

Author

vltaexaminer

VLTA Examiner