Cyber-Insurance: Your Guide to Buying with Confidence

Description

As we move through 2016, most title agents will agree that cyber protection has become a necessary evil. It is yet another cost to add to the insurance portfolio that seems to be getting more expensive each year. Unfortunately, the cost for adequate protection may not be going down any time soon.

One of the biggest challenges when shopping for cyber insurance is to understand exactly what you are buying. The policy forms differ drastically from carrier to carrier and pricing is all across the board. To determine what kind of coverage you need, start to think about what your officeâ??s specific exposures may be.

Here are a few of the claim scenarios we have come across in the title industry. Ask yourself if you could see yourself, or your employees, falling victim to any of these scams.

1. **Phishing or social engineering scams**: An employee receives revised wire instructions from a sellerâ??s agent, attorney or lender. A few days later, she discovers the revised instructions came from a fraudulent party and the money has since left the country. The bank acted according to instructions from an authorized representative of the Title Agency and denies any liability for the lost funds.
2. **Funds transfer fraud**: A hacker gains access to your online banking system and successfully transfers money out of the escrow/operating account. Litigation ensues with the bank, while your account remains overdrawn. Assuming the role of fiduciary, you are responsible for safeguarding your clientâ??s funds.
3. **Extortion**: You come in to the office and the computer systems are completely locked down. No one can gain access. Your systems (including your clientsâ?? non-public information) are being held ransom. You will not gain access to the system and your clientâ??s information may be made public unless you make a ransom payment.
4. **Privacy liability**: An employee is traveling and leaves their laptop in the airport. The laptop contains non-public information on hundreds of clients spanning multiple states. You must comply with each stateâ??s specific regulations governing the breach response and notification. Some states require notification in as little as 24 hours. You may be required to provide credit monitoring as well.

These scenarios are just a few examples of cyber security breaches we have seen affect the title industry. The frequency and severity of cyber-related claims continues to grow.

With this emerging market, many insurance carriers are jumping at the chance to provide cyber insurance. There are many options available, but it is critical to discuss the coverage differences with your broker. For example, an E&O endorsement will not provide the same level of coverage as a full cyber liability policy. Similarly, a basic (unendorsed) cyber policy may not provide appropriate coverage.

As cyber crime threats continue to increase, the insurance industryâ??s response will also evolve. The policy forms and endorsements are changing so rapidly and, as you can see, it is not easy to compare quotes. Because coverage and endorsements vary from carrier to carrier it is nearly impossible to shop based on price alone. The good news is that these policies offer room for negotiation â?? as long as you (or your broker) know what to demand. While this constant state of change leads to a complex market and a variety of products, you cannot afford to shy away. It is critical to talk to your broker and find the coverage that is right for your organization.

*This article was intended for informational purposes only. Please thoroughly discuss your potential liability with your attorney and the coverages available to you with an insurance broker that is knowledgeable on the subject of cyber liability insurance.

Category

1. Cybersecurity

Date Created
2017/12/18
Author
vltaexaminer