Cyber Insurance Is The Answer

Description

Virginia is an industry leader in the development of legislation regarding e-closings and remote notarizations. Virginia is only one of two states in the country (the other being Montana) that has allowed for online notary e-closings. While we wait for lawmakers in the rest of the country to catch up, Virginia Land Title professionals must maintain a strong focus on cyber security.

What can you do to keep your company safe?

There are a few simple steps you and your team can put in place to strengthen your defense against cyber attackers.

- Change passwords often. Too many of us use the same password across different channels year after year. You may consider using a password manager to assist with generating and storing strong passwords.
- Utilize multi-factor authentication. You can make it more difficult to breach your system by adding another layer of authentication on top of your username and password.
- Encrypt, encrypt, encrypt â?? making your data impossible to read. Encrypt e-mails, especially when sending sensitive data. Also, encrypt data stored on your server and on the cloud.
- Train your employees! Human error is a major factor in cyber breaches across the country. Train and test employees regularly so that they fully understand cyber security is a team effort.
- Perform regular software updates. Outdated software is another weak link in the security chain; keep all computers and servers up to date with security patches.

A prevalent threat is the use of social engineering (also known as business e-mail compromise or deceptive fraud).

This tactic is even simpler for thieves to execute, as it requires no technical sophistication. They may only use public information or material obtained from social media to deceive the victim. Social engineering is rampant but can be easier to detect if you know some warning signs.

- Question the senderâ??s e-mail address and domain â?? are they familiar? Hover your mouse over the senderâ??s name to see the full e-mail address.
- Is the e-mail unexpected? Does it contain a link or an attachment?
- Who else is copied on the e-mail? Does it make sense for an e-mail to be sent to that particular group of people?
- How is the grammar?
- When was this e-mail sent? Was it within normal business hours or in the middle of the night?
- Are they requesting a payment? A change to wire instructions?

Unfortunately, even when cyber security is a priority, your business can never be one hundred percent secure.

A few exposures are common to any business, including the theft of NPI (non-public personal information), rogue employees, extortion and theft of funds from operating accounts. Any business with a website or social media presence has potential liability for personal / advertising injury or intellectual property infringement. For title professionals, the complexity and number of players in the home-buying process introduces different cyber exposures at each step.

Settlement agents have the unique exposure of the theft of escrow funds. Initially, settlement agents were targeted by receiving a request for a wire after the settlement had occurred, instructing them to wire the seller proceeds and place a stop payment on the check. More recently, we have seen a shift to consumer-targeted phishing scams. In these scams, the homebuyer is contacted prior to closing and told to wire their down payment (or entire payment, for cash deals) according to wire instructions included in an e-mail. Since the potential thieves are purporting to be the settlement agent, that is who the homebuyer files a lawsuit against, typically alongside any other professional who was a party to the transaction.

Given homebuyers unfamiliarity with the process, this has been incredibly successful. Thus, if you cannot achieve total security within your own office and you cannot prevent a homebuyer from sending their money to a thief, how can you possibly protect yourself?

Cyber Insurance is the answer.

Unfortunately, a breach can be extremely costly and has a very real possibility of putting you out of business. A good cyber policy can cover a wide range of potential issues; including theft of data, notification costs, forensic investigation costs, fines and penalties associated with a breach, media liability, system business interruption costs, data recovery costs, extortion demands, theft of money from your accounts and theft of money from your clients. The right policy can provide both an expert partner (to guide you through the necessary steps to take following a cyber security breach) as well as financial assistance in dealing with a confirmed cyber-attack.

Itâ??s important to make sure your policy has coverage for the exposures you face in your particular role in the settlement process. Coverage varies drastically from carrier to carrier, so getting an â??off-the shelfâ?• cyber policy may not be sufficient. Work with a broker who understands what you do and has the ability to access carriers that offer the coverage you need. Take care of yourself, your your clients.

Kaitlin Kelly *is an owner of Fran Kelly Professional Liability, LLC. For the past ten years she has been an insurance producer at Fran Kelly Professional Liability which focuses specifically on Professional Liability products for Title Industry clients. She provides continuing education to Title Professionals in PA, OH and NJ on professional and cyber liability insurance. She graduated from*

University of Pittsburgh with a degree in Finance and a minor in Economics.

Category

1. Cybersecurity

Tags

1. featured

Date Created
2018/03/01
Author
vltaexaminer