Insurance // Commercial E&O

Real Estate and Cyber Risks

Did you know that...

- Cyber crooks target smaller and medium sized firms. In fact more than 50% of businesses have experienced a cyber-attack in the past year according to a study of businesses conducted by research firm Zogby Analytics for HSB.
- The cost of cyber risk events is significant. 72 % of the small to midsized businesses that said they were hacked spent $5,000 or more. And 38% of those hacked spent over $50,000 to respond.
- Virtually all small to mid-sized businesses are at risk because they have computers and portable devices, store electronic data, retain people's private information and are dependent on the Internet.

It's clear that cyber security is a risk for all firms – regardless of industry, size, or location. If you have data, you have cyber risks. Consider the following loss scenarios to see how real estate professionals could potentially be impacted by a cyber incident.

Scenario 1
Cyber criminals were able to breach a real estate agent's email account, accessing the personally identifying information of over 250 clients of the real estate firm where the agent was employed. Using the breached personally identifying information and access to the real estate agent's email account, the criminals crafted a fraudulent email instructing one of the firm's clients to send payment for a real estate purchase to a bank account controlled by the criminals. Relying on the email, the buyer made the payment. The email account hack and data breach were not discovered until the buyer reported that it had wired the necessary payment, and the firm realized it had no record of it. The firm was proactive in addressing the data breach, remediating its systems and notifying the defrauded buyer and all of the other affected individuals. But at the end of the day, the one client who paid the cyber criminals was still out their $25,000 down payment, which they sued the real estate firm to collect.

Coverage applied: Data Compromise Response Expense, Data Compromise Defense and Liability, CyberOne™ Computer Attack.

Scenario 2
Hackers gained access to the servers running databases behind the website of a small real estate firm. The firm learned of the attack when Google notified it that the site had been infected and blocked access to it. An outside IT firm was hired to find and delete the malicious code—three times. The first two fixes lasted only a week before the infection recurred. Insured losses: IT work and lost business $16,000.

Scenario 3
The customers of a real estate agency received strange emails appearing to have come from the firm. Worried, the office manager called an outside IT consultant who investigated and fixed the problem. An agent's computer had been infected by a virus, but it was easy to remove. The consultant left a bill for $200. Several weeks later, the office manager received a lawyer's letter alleging that a former customer had been infected by a virus received in an email message sent by an agent of the firm. According to the letter, the former customer had suffered a variety of different kinds of harm related to the virus, and had incurred significant costs to have the virus removed. The real estate firm engaged its own attorney, and by the time the matter was resolved, the firm paid $30,000 to settle the dispute with the customer and $18,000 for its own attorney.

Scenario 4
It's no secret that real estate agents keep files on their clients which contain a cyber criminal's treasure trove of personally identifying and financial information. This makes real estate firms prime targets for thieves. A burglar broke into a real estate office and stole a computer with the records of 800 clients. The clients were in multiple states as some were relocating to the area, and the firm needed assistance complying with the variances of state data breach notification requirements. Clients were notified and provided with credit monitoring, identity theft restoration and other services. Cost of notification and services: $28,000.

Continued

AXA XL Solution: CyberOne™ and Data Compromise

We understand these risks and offer comprehensive cyber coverage to help small firms respond and recover from cyber attacks. Our cyber coverage includes:

- **CyberOne™ coverage** helps pay for the costs associated with restoring data and computer systems as well as protects against third-party liability that may arise from a failure of a system security.
- **Data Compromise coverage** is designed to help clients respond to the financial burden and service obligations of a data breach.

Included Resources and Tools

Coverage includes access to an online resource with information about training, best practices, and risk management tools for cyber exposures.

With this information, insureds can assess their risk and develop an effective response plan to help protect their client relationships and business reputation in the event of an attack.

CyberOne™

Computer Attack Coverage

- Coverage is triggered by a computer attack
- An unauthorized person gaining access to the insured's computer system
- A malware attack
- A denial of service attack
- In the event of a computer attack, CyberOne™ pays for:
  - Data re-creation (from non-electronic sources)
  - Data restoration (from electronic sources)
  - Loss of business income
  - Systems restoration

Network Security Liability Coverage

- Coverage is triggered by a network security liability suit – a civil proceeding, an alternative dispute resolution proceeding, or a written demand for money alleging that a negligent failure of the insured's computer security allowed one of the following to occur:
  - The breach of third party business data
  - The unintended transmission of malware
  - A denial of service attack in which the insured unintentionally participated
- In the event of a network security liability suit, CyberOne™ covers costs of defense, settlement, and judgment. Defense is provided within the coverage limits.

Limit and Deductible
Computer Attack

- $100,000 annual aggregate limit
- $2,500 deductible per computer attack

Network Security Liability

- $100,000* annual aggregate limit
- $2,500 deductible per network security liability suit

Data Compromise

Response Expenses Coverage

- Coverage is triggered by the discovery of the breach by the insured. A data breach includes:
  - Theft of electronic files or physical files
  - Accidental loss or release of files
  - Voluntary release due to fraud
- In the event of a data breach, Data Compromise coverage pays for:
  - First-party expenses in responding to a personal data breach
  - Outside legal counsel review, forensic IT review, notifications to affected individuals, credit monitoring and identity restoration services to affected individuals

Defense & Liability Coverage

- Coverage offers legal defense cost and liability coverage as part of the program to protect businesses from lawsuits filed by consumers upset about a data breach when their private information is exposed.

Limit and Deductible
Response Expense

- $100,000 annual aggregate
- Sublimits: Any one Personal Data Compromise
  - Forensic IT review $10,000
  - Legal review $10,000
  - Named malware $50,000
  - Public Relations service $5,000
  - $2,500 deductible any one Personal Data Compromise

Defense and Liability

- 100,000* annual aggregate
- Sublimits: Named malware $50,000 any one Personal Data Compromise
- $2,500 deductible each Data Compromise Suit

Real Estate ProtectionPlus
Exclusively provided by Pearl Insurance

PEARL® INSURANCE

ALABAMA REALTORS

Contact Pearl Insurance to learn more.

www.pearlinsurance.com
855.465.0200

* In Arkansas, Louisiana, Montana, New Hampshire, Oklahoma, South Dakota and Vermont, the $100,000 Network Security Liability limit is replaced with a $50,000 Network Security Liability Limit and a $50,000 Network Security Defense Limit.

CyberOne™ is a trademark of The Hartford Steam Boiler Inspection and Insurance Company. © 2017 The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved. This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form.

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details. XL Catlin, the XL Catlin logo and Make Your World Go are trademarks of XL Group Ltd companies. XL Catlin is the global brand used by XL Group Ltd's (re) insurance subsidiaries. In the US, the insurance companies of XL Group Ltd are: Catlin Indemnity Company, Catlin Insurance Company, Inc., Catlin Specialty Insurance Company, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., and XL Specialty Insurance Company. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions. Information accurate as of December 2017.

2410_12/2017

201328-A1-PP-EO-FLYR-AL