

Cybersecurity Risks For Real Estate Professionals? They Are Alive And Well

by Gary Strong, Esq.

We have all heard about the massive data breaches at Target, Home Depot, and more recently JP Morgan Chase. As these data breaches have grabbed the biggest headlines, the media has rightfully focused on the staggering effects on consumers and response costs for the companies. Risks associated with data security and data breaches only continue to grow, and impact a variety of industries worldwide.

One would think that the real estate industry should be immune from cyber risks; however, increasing reliance upon technology within the real estate sector and the fact that real estate firms are creating, using, storing and sharing more personal and sensitive information should change that view. Because cyber risks can exist in many forms — from malicious cyber-attacks, to negligent employees, to unmanaged data sharing with vendors — real estate professionals must take a serious look at their cyber risk exposures and how they are managed.

Examples of Data Breaches

Property managers, brokers/agents, title agents, developers, appraisers, multi-service real estate firms and others may have significant amounts of confidential third-party information, either in the form of personally identifiable information or confidential corporate information; rental applications, credit reports, leases and rental agreements contain personal information of applicants and tenants — precisely the type of information targeted by cyber criminals.

The costs associated with a cyber-incident can be significant because in order to investigate and remediate a breach, forensic companies must often be hired to identify the source of a data breach. Expenses associated with notifying individuals whose confidential information may have been compromised can also be significant. Responding to breaches may also negatively impact productivity, drawing on crucial company resources in an attempt to respond quickly and effectively. Finally, network interruption could lead to loss of income and generate unnecessary additional expenses for real estate firms who rely on their network to conduct business. Combined, these amounts can reach hundreds of

thousands or even millions of dollars, damaging the balance sheets of larger real estate firms and potentially crippling smaller real estate businesses.

Protecting Real Estate Agent's and Brokers from Cyber-Risks

Here are some ideas for what brokers can do now to protect themselves and their agents from being hacked:

1. Encrypt e-mail. Installing encryption software, such as Gnu Privacy Guard, will prevent some hacking threats.

2. Use a Virtual Private Network. For about \$6 or \$7 a month, you can use a VPN, which makes sure all your communications are automatically encrypted and tunnel through a protected network instead of through the servers accessible to hackers. Private Internet Access is a popular VPN option.

3. Encourage agents to use a business e-mail address. Many real estate agents use their personal e-mail accounts. However, using the private domain of an agency is much safer than using a Yahoo or Gmail address.

4. Secure all documents in digital vaults which are like safety deposit boxes on secure servers where everything is automatically encrypted all the way to the destination.

5. Buy a cyber liability insurance policy. According to the National Association of Insurance Commissioners' website, new cyber liability insurance is "expected to grow dramatically over time as businesses gradually become more aware that current business policies do not adequately cover cyber risks." This type of insurance can cover such issues as liability for security or privacy breaches or providing credit monitoring services to affected consumers.

Potential Officer and Director Liability

While taking these steps will provide some protection, individual officers and directors may still face exposure in the form of shareholder derivative lawsuits. These type of lawsuits allege that directors breached their fiduciary duties to their shareholders/investors by not doing enough oversight to ensure that controls were in place to guard

the company against a data breach. The liability risk for officers and directors extends to the protection of any commercially sensitive information, including confidential customer information, customer lists, trade secrets, competitive business information, etc., for which the directors may owe a fiduciary duty to owners, or a contractual duty to clients, to protect and to keep confidential (from both external attacks and internal/employee misappropriation/negligence).

If there is a data breach and material loss of sensitive information, investors may start asking whether officers and directors did enough to protect critical business information (both the company's and the company's clients).

In sum, while the electronic age has some obvious advantages, professionals like real estate agents/brokers must be aware of the potential liability on the macro level (making sure the company has adequate safeguards in place) as well as the micro level (making sure employees are aware of the threats and performing their day to day tasks in a secure fashion. ♦

Gary Strong, Esq. is Senior Associate with Seiger Gfeller Laurie, LLP. He specializes in defense of E&O claims against Real Estate Professionals as well as advising client(s) of cyber liability issues. He can be reached at 609/375.2035 or via email at gstrong@sgl-lawgroup.com.

Wayne D Kenny
President
wkenny@abcsafetyfire.net

ABC Safety Fire Inc
Sprinklers-Fire Extinguishers-Kitchen Suppression

750 Fairfield Ave
Kenilworth, N.J. 07033


908-259-9200
Fax 908-259-9021
www.abcsafetyfire.com

• AUTO
• TRUCK
• HOME
• BUSINESS

ABNET INC.
INSURANCE SERVICES

JULES BORRUS
SALES ASSOCIATE

44 STELTON RD. - SUITE 120
PISCATWAY, NJ 08854
TEL: (732) 424-0121
FAX: (732) 424-0158
CELL: (908) 839-0052

 borruscommre@aol.com • www.abnetincnj.com