The Real Estate Industry's Hidden Risk: Network Security And Privacy Liability

Frank DeLucia, HUB International Northeast and John Farley, HUB International East Region

2014 was the year that cyber risk became a national, highly publicized conversation. High profile data breaches at Target, Home Depot and Chase, among other well known institutions, forced organizations across multiple industries to take a hard look at their potential vulnerabilities in network security and privacy liability. Most experts agree that certain industries such as Healthcare, Retail and Financial Services are at higher risk than others since they collect and store a vast amount of sensitive data.

The real estate industry is usually not categorized as "high risk" but that risk profile could change and there are many exposures that cannot be ignored. **Real estate professionals routinely obtain, store and transmit personally identifiable information, including social security numbers and financial records. This data is often obtained from credit reports, rental applications, leases and rental agreements.**

That data collection imposes legal duties on the real estate industry to safeguard it. Should it be compromised, real estate professionals could find themselves in the same situation as the organizations we all read about in the news. Legal fees, IT forensics expenses, notification and credit monitoring costs and investigations from government authorities would be expected. The financial impact and reputational damage could be significant. In fact, **according to the 2014 Ponemon Institute Cost of Data Breach Study, the average cost to a company was $3.5 million, 15% more than what it cost last year.**

The real estate industry can start addressing this risk by asking some basic questions. What data do I collect? Why do I collect it? Where is it stored? Who has access to it? How well is it protected? When and how should it be purged? What will we do if it is accessed by an unauthorized party?

Cyber Liability Insurance, also known as Privacy/Data Liability Insurance, is a rapidly evolving product in today's marketplace. In fact, **Cyber Insurance is the fastest growing coverage in the insurance industry, according to The New York Times.** The basic elements of a Cyber Liability insurance product can include coverage for a number of expenses associated with breach including legal expenses, notification expenses, regulatory fines and penalties, credit monitoring and public relations expenses.

Below is a brief overview of some popular Cyber Liability insurance coverages available to protect your real estate business. Your broker can help you navigate through the options available to ensure your policy provides adequate protection.

• Privacy Liability - Covers loss arising out of the organization's failure to protect sensitive personal or corporate information.

• Network Security Liability - Covers any liability of the organization arising out of the failure of network security, including unauthorized access or unauthorized use of corporate systems, a denial of service attack, or transmission of malicious code.

• Internet Media Liability - Covers infringement of copyright or trademark, invasion of privacy, slander, plagiarism or negligence arising out of internet content.

• Privacy Breach Costs/Data Breach Fund - Covers expenses to notify customers whose sensitive personal information has been breached, to retain a computer forensics firm to determine the scope of a breach, and to obtain legal, public relations or crisis management services to restore the company's reputation.

• Network/Cyber Extortion - Covers extortion monies and expenses associated with a criminal threat to release sensitive information or bring down a network unless payment is received.

• Digital Asset Loss - Covers costs incurred to replace, restore or recollect data which has been corrupted or destroyed as a result of a network security failure.

• Business Interruption - Covers loss of income and extra expense arising out of the interruption of network service due to an attack on the insured's network.

• PCI Fines and Costs - Pays amounts owed under a merchant services agreement for non-compliance with PCI Data Security Standards.

Cyber attacks are the fastest growing crimes in the world and most standard insurance products do not address this exposure. Don't leave your business vulnerable and unprotected; your insurance advisor can help you conduct an assessment to identify your company's risk profile so you can take appropriate actions to reduce those exposures and find a coverage plan designed to meet the needs of your company.

Frank DeLucia
Senior Vice President
HUB International Northeast
Tel: 212-338-2395
Frank.delucia@hubinternational.com
www.hubdelucia.com

John Farley
Cyber Risk Practice Leader
HUB International East Region
Tel: 212-338-2150
John.farley@hubinternational.com