THE HUNTON GAMES

Real Estate Is Not Above the (Cyber Attack) Risk

At one time, commercial real estate players were considered less at-risk for cyber attacks because they maintain comparatively less personal information and intellectual property than financial, health care and retail companies. Consequently, CRE folks have been slow to invest in cybersecurity and insurance for cyber risks. Being soft on cyber has also meant that some CRE players have outdated traditional coverages, like crime policies, that do not address cyber risk variants like fraudulently induced money transfers. But as buildings get *smarter* through integrated technology, as regulators enhance enforcement against any business that touches sensitive personal information and as CRE pros engage in increasingly complex financial transactions, the need for responsive cyber and crime insurance cannot be ignored. Simply put, real estate is not above the risk, and it is time to act accordingly.

The Real Estate Industry Is a Real Cyber Target With Real Insurance Needs

The real estate sector is a growing target for cybercriminals. KPMG reports that one-third of real estate firms have experienced a cybersecurity event themselves or at one or more of their properties in the last two years, though that number is likely higher since half of respondents also reported that they were not adequately prepared to prevent an attack (and, thus, may not know if they were infiltrated).

CRE firms are attractive targets because of their access to both data and money. Data—such as personal information, blueprints, building technology and financial information—can be sold or used for future exploits. Money can be skimmed from tenant and vendor accounts or credit cards and extorted directly thanks to ransomware. Last year, for example, an Austrian hotel paid a hefty ransom after its computers were hacked; and just this month, property management firm BNP Paribas Real Estate reported a ransomware attack that took down most of its global systems.

Walter Andrews

Jennifer White

For these types of risks, the right cyber insurance policy makes all the difference. First-party cyber insurance typically covers lost business income, extra expenses, forensics and notification costs associated with investigating and resolving a breach. Third-party cyber coverages pick up the tab when regulators come knocking, or third parties seek personal damages subsequent to an attack.

For other losses like stolen money, however, cyber insurance falls short. Instead, CRE companies must revise traditional insurance policies, particularly crime coverage.

The Right Crime Coverage Can Protect You From Yourself

Most crime coverage now includes endorsements to cover loss caused by social engineering, where cybercriminals deceive and manipulate employees into sharing confidential information used to steal money or trick employees into unintentionally facilitating a theft. Cybercriminals often pose as legitimate vendors, customers or employees and may use accurate business information (gathered by accessing and watching email traffic) to achieve the ruse.

However, even the right crime coverage will need to be tailored to your business model. For example, last week, a federal court in New York held that a crime policy covered $4.8 million lost to cybercriminals who tricked employees into wiring the funds offshore by fabricating realistic emails from the company's president. See Medidata Solutions, Inc. v. Federal Ins. Co., 15-CV-907 (S.D.N.Y. July 21, 2017). The Court held that cybercriminals gained unauthorized access to Medidata's "computer systems," as the policy required, by manipulating computer code to mask the imposter's identity. Luckily for the company, the critical policy definitions reflected the reality of its business; "computer systems," for example, included facilities "utilized by" the insured, which was important because Medidata relied on a third party to facilitate the violated email accounts. Details like these are important to CRE insureds, which often rely on vendors to host web applications, organize customer data, or facilitate financial transactions. Thus, obtaining coverage is the first step; tailoring it is the next.

Attention to Insurance Matters

For most CRE companies, it is only a matter of time before a cyberattack takes out a critical business program or steals thousands from accounts payable. With the proper policies in place, CRE firms can minimize the institutional and financial pain associated with such attacks. Ideally, those policies should be tailored to CRE risks, using skilled brokers and coverage counsel who understand the industry. But before any of that can occur, the CRE industry must first recognize its status as a legitimate cyber target and subject to the same risk afflicting all major industries.

Walter Andrews is a partner at Hunton & Williams, and Jennifer White is an associate. They can be reached at wandrews@hunton.com and jewhite@hunton.com, respectively.