New York Real Estate Journal
nyrej
THE LARGEST COMMERCIAL/INVESTMENT REAL ESTATE NEWSPAPER IN THE STATE
Reprint | nyrej.com | Tuesday, April 4, 2017

Ignore cyber risks at your own peril: Real estate industry must implement the best practices

John Cooney
Ruskin Moscou Faltischek

Benjamin Weinstock
Ruskin Moscou Faltischek

Cybersecurity is one of today's toughest business challenges. Regrettably, it has been largely ignored by real estate owners and operators. Headlines have involved financial institutions and retailers (JPMorgan Chase, Home Depot, Target) but the real estate industry is not immune and faces the same cyber risks. Identity theft, the most common cyber risk, cost 15.4 million consumers over $16 million in 2016, and it cost the hacked companies significantly more. The real estate industry must recognize these risks to avoid becoming cyber-victims with multimillion-dollar liabilities for damages and curative actions.

Managing cyber risks is different than typical risk management in real estate. The technology and nomenclature is new and daunting, if not outright intimidating. Nevertheless, owners and operators need to become informed, assess their vulnerabilities and take pre-emptive measures to avoid ruinous liability.

The real estate industry contains the same treasure trove of information often targeted in cyberattacks: owners and operators collect and maintain personal, banking, credit card and other financial information about their tenants, financial transactions and vendors. In fact, real estate transactions have already been a favorite target of hackers.

Within the last year, hackers have aggressively targeted closing funds, tenant security accounts and earnest money deposits by penetrating email accounts and supplying false bank wiring instructions. To pull off this fraud, the hacker usually attacks and monitors an email account to learn the timing of deals and identities of all involved parties. Once inside, a hacker can effectively assume the identity of an agent, attorney or executive and provide credible wire instructions to steal funds. Unfortunately, once the funds are sent pursuant the false wire instructions, there is almost no chance at recovery.

Cybersecurity is one of today's toughest business challenges. Regrettably, it has been largely ignored by real estate owners and operators.

Besides transactional risk, owners and operators, including property management firms, maintain very sensitive personal and financial information such as bank accounts, credit reports, Social Security numbers, drivers' licenses, and birthdays. Theft of this information exposes the repository and owners of the information to reputational damage and significant associated costs, such as damages and protective measures for injured consumers.

For instance, the New York State Information Security Breach and Notification Act requires notice to residents when a hacked account contains a combination of name, Social Security number, driver's license, and financial account numbers. In addition, in New York the Office of Attorney General, State Police and State Consumer Protection Agency must be informed. Dealing with these agencies will result in expensive legal and technical expert fees.

The increase in cyberattacks has resulted in an increase in lawsuits and regulatory investigations targeting senior management and their actions, or lack thereof. Recent lawsuits and investigations include claims that a business failed to take even the most basic security precautions, such as changing passwords, to protect personal information. The facts are often damning when a business fails to assess its vulnerabilities, update its data security systems and policies, detect breaches, and respond to incidents in a meaningful, timely manner. There are simple and basic steps that every property owner and operator can take now, before a breach, to mitigate liability from a cybersecurity incident. Experienced attorneys who understand the cyber risks and how to minimize losses can guide the client in the process.

The same due diligence applies when selecting a vendor. As many high profile breaches have demonstrated, vulnerabilities of third party vendors can be used to launch an attack on the host company. This is especially important when contracting a third-party data or property manager to process credit card payments, manage package deliveries, or track maintenance requests from tenants. Imagine a hacker finding out that you will be in Australia for the first two weeks of April. Therefore, the owner must scrutinize the vendor's contract and technology to avoid assuming open-ended and costly cyber risks. Is the vendor collecting and storing personal, sensitive information about tenants? Is the vendor taking adequate steps to protect credit card information? Does the vendor assume responsibility and costs for any breach or attack originating through its system? Does the vendor have adequate cyber-insurance? Is the owner a named insured? This is just a small sampling of the due diligence required before hiring any third-party vendor.

As cyberattacks continue to multiply, the real estate industry must understand that cyber risks must be addressed and managed with the same attention and care as any other major risk. At the minimum, a multi-pronged approach should be adopted to understand the different issues, assess vulnerabilities and implement best practices.

John Cooney, Esq. is a partner and chair of the cybersecurity and data privacy practice group and Benjamin Weinstock, Esq. is a partner and co-chair of the real estate department at Ruskin Moscou Faltischek, Uniondale, N.Y.