Cybersecurity Issues for the Commercial and Industrial Real Estate Sectors: Are Your Leases and Other Agreements Protecting Your Assets in a Digital World?

Matthew J. Schiller and Mitchel S. Kay
Greenbaum, Rowe, Smith & Davis LLP Client Alert
March 2018

Advances in technology have the potential to be great disruptors in nearly every industry. The commercial and industrial real estate sectors are no exceptions. The positive changes that come with such advancements tend to be accompanied by increased risk. The Counselors of Real Estate, an international organization of high profile property professionals from all sides of the industry, recently identified technology as one of the "Top Ten Issues Affecting Real Estate" in 2017-2018, commenting that technology has "revolutionized the property industry, with an unprecedented wave of innovation changing the way real estate is bought, sold, and managed." The group goes on to note that "the pervasiveness of hackers–and the threat that internet intrusion presents to businesses, product functionality and homes–makes cybersecurity a top priority for real estate business owners and practitioners."

While industries such as financial services, retail, travel and hospitality have been quicker to identify and implement the benefits of new technology, the real estate industry as a whole has been trying to catch up.

Many owners of commercial and industrial properties have already invested in technological buildouts and "smart" building management systems (BMS), a trend that continues to gain traction. A smart BMS utilizing Internet of Things (IoT)/smart technologies can create a platform to control functions such as lighting, building access and security, heating, ventilation and air conditioning. Real estate companies are also embracing the use of technology via social media, cloud/SaaS (software-as-a-service) solutions, and mobile platforms. These initiatives often provide cost-saving measures that simultaneously improve the tenant experience and create a win-win scenario for all concerned.

However, these technologies create a new sphere of vulnerabilities by increasing the number of channels through which personal information and confidential data can be accessed and stolen. Unauthorized access to sensitive information through building management and information systems can expose building owners, landlords, tenants, property managers, third party vendors and customers/clients to potentially catastrophic economic and reputational damages.

Importantly, the stakeholders of commercial and industrial real estate properties must look beyond the physical security of their assets. They must consider and take steps to protect against a hacker's ability to target their properties through building management systems, employee devices (e.g. mobile phones,

laptops and tablets), online payment and point-of-sale systems, mobile and web applications, internal and external webservers, networks and the cloud, and open Wi-Fi access.

Ensuring that proper cybersecurity protocols are in place, and engaging the assistance of knowledgeable IT consultants are key pieces of the puzzle. Having updated internal policies and training for staff, as well as instituting a business continuity plan (BCP) to strategize and prepare for cyber risks, are also of paramount importance. Protective provisions in contracts and leases should address the risks associated with current and emerging technology trends. Key provisions include: (1) insurance (including cyber liability insurance); (2) indemnification; (3) representations, warranties and limitation of liability; (4) performance of supplier; (5) security event/security notification; (6) maintenance and upgrades; (7) maintenance services with service level credits and (8) casualty/condemnation.

If you would like to learn more about the liabilities associated with the growth of technology in the commercial real estate sector, or would like to discuss the modernization of new or existing agreements to help mitigate the risks associated with cyber-breaches, please contact the authors of this Client Alert, **Matthew J. Schiller** and **Mitchel S. Kay**.