THE COUNSELORS OF REAL ESTATE®

REAL ESTATE ISSUES®
Published by The Counselors of Real Estate®

Cybersecurity Interruptions

Volume 46, Number 11 - August 29, 2022 • Written by: Mr. Tom Shircliff, CRE

Photo: Gorodenkoff/Shutterstock.com

Mr. Tom Shircliff, CRE

is an entrepreneur and executive with broad experience in Fortune 500 management, small business and venture capital-funded startups including local, regional and national roles. Since co-founding Intelligent Buildings, LLC, he has become a recognized expert in the field of commercial real estate technology consulting and risk management. Since 2004, Intelligent Buildings has been a leader in commercial real estate smart building consulting, assessments and managed services.

Cybersecurity Interruptions was listed as the #9 issue in the 2022-23 Top Ten Issues Affecting Real Estate® by The Counselors of Real Estate®.

> ***"This is not a so-called smart building or Internet of Things (IoT) problem, which continues to add to risks, but rather a 40-year build-up as our main systems (e.g., HVAC, elevator, lighting, access control, parking) have all required computers, networks, and Internet connections since the 1980s."***

We are in a new era of cybersecurity risks in commercial real estate, driven by decades of technological advances that impact all buildings' physical and environmental functionality. There are material risks for investors, owners, operators, and occupants. Risks include insurance gaps relating to nation-state attacks and for-profit ransomware, as well as from ill-equipped building managers and contractors.

Insurance carriers and brokers increasingly deny cybersecurity insurance coverage. When you can get a policy, the premiums skyrocket, and there are gaps and exclusions in existing policies. Often, cybersecurity incidents in building control systems are not addressed in property and casualty (P&C), general liability, and cyber riders and can result in litigation as well as the aforementioned exclusionary language emerging notably in P&C. Directors and Officers (D&O) insurance is now rising in importance with some cybersecurity lawsuits against individuals and recent SEC Cybersecurity disclosure proposals.[1]

This is not a so-called smart building or Internet of Things (IoT) problem, which continues to add to risks, but rather a 40-year build-up as our main systems (e.g., HVAC, elevator, lighting, access control, parking) have all required computers, networks, and Internet connections since the 1980s. These IT elements are necessary to provide building-wide control between devices and floors as well as remote maintenance and updates. Notwithstanding those multiple decades of technology inundation, there have never been suitable technology or cybersecurity skill sets in the entire CRE value chain from design to development and management. Therefore, the problem is systemic and pervasive throughout the entire industry, which is unfortunately now on full display in a global era of cybersecurity awareness.

More recently, there has been a steadily intensifying cybersecurity theme from state actors such as Russia (publicly) and Iran (in secret documents) and for-profit hackers that all target critical infrastructure in the West. This is not only power plants and dams but also commercial real estate and all non-single-family use types. In one specific instance, Russian malware was recently discovered in REIT HVAC systems only one week after the U.S. government warned of the malware by name and country of origin.[2] Iranian documents mention specific system and manufacturers of HVAC, lighting, and metering systems when stating their malicious intentions for commercial real estate.[3] These real estate targets include corporate office properties, banks, schools, hospitals, public venues, and more. The Boston Children's Hospital HVAC contractor was ransomed by international hackers and created intense concerns.[4]

Consequences can include life safety issues, equipment replacement, unmitigated access to corporate networks, full-building downtime, and significant brand damage. We are entering the perfect storm from the confluence of decades of tech buildup, lack of skill sets, cultural ignorance, savvy bad actors, and a dependency on commercial real estate as critical infrastructure. This impacts all stakeholders but can be influenced most broadly by investors and owners as their policies and requirements can be mandated downstream to asset managers and property managers for assessments, policy enforcement, and active monitoring.

Endnotes

[1] "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," U.S. Securities and Exchange Commission (March 9, 2022). https://www.sec.gov/news/press-release/2022-39

[2] "Russian Malware Attack On Commercial Real Estate," Intelligent Buildings, LLC. https://www.intelligentbuildings.com/likely-russian-malware-attack-on-commercial-real-estate/

[3] Eduard Kovacs. "Leaked Files From Offensive Cyber Unit Show Iran's Interest in Targeting ICS," SecurityWeek, Wired Business Media (July 29, 2021). https://www.securityweek.com/leaked-files-offensive-cyber-unit-show-irans-interest-targeting-ics

[4] "Exclusive: Attack on HVAC vendor gave threat actor access to Boston Children's Hospital," DataBreaches.net (August 17, 2021). https://www.databreaches.net/exclusive-attack-on-hvac-vendor-gave-threat-actor-access-to-boston-childrens-hospital/