REAL ESTATE ISSUES®

Published by THE COUNSELORS OF REAL ESTATE®

Cybersecurity of Building Technology: Smart Cities and Smart Buildings Require Smart Protection

By Marie-Noëlle Brisson, CRE; Dan Doggendorf; and Michael Savoie, Ph.D.

Volume 43, Number 1
March 5, 2019

Photo: Rawpixel.com/Shutterstock.com

Continued from Volume 42, Number 2 and Number 10.

INTRODUCTION

Cybersecurity has become a major issue for commercial real estate in many more ways than previously anticipated. Ongoing vigilance – making security a part of the culture of your organization – is the best defense against a data breach. This is the third in a series of articles addressing cybersecurity issues in commercial real estate.

In the first article, we discussed the value of data as a corporate resource and how processes and procedures need to be put in place to protect it. By focusing on vulnerabilities inside and outside the organization, minding third party interactions, educating your employees, and recognizing that security is everyone's job, companies can create an environment that is "security aware" and vigilant against unwanted intrusions.

In the second article, we explained how data governance has become a critical issue, why a data life cycles needs to be defined and should be everyone's concern, and explored how data should be handled and protected. Data protection is only as strong as the weakest link in the process.

ABOUT THE AUTHORS

Marie-Noelle Brisson, CRE, is Senior Advisor and a Managing Partner at SONRO Real Estate Services, bridging the gap between urban planning and commercial real estate, helping companies and cities optimize under-utilized assets and urban spaces. As a certified non-executive director, she focuses on cybersecurity and data governance issues.

Dan Doggendorf is the Founder/Principal Advisor of Pro4:Six Consulting, a cybersecurity, compliance, and technology advisory firm addressing all stages of the corporate lifecycle.

Dr. Michael J. Savoie, Ph.D, is CEO of HyperGrowth Solutions, Inc, a company focused on integrating disruptive technologies with business (www.hgsonline.com). Dr. Savoie is also a visiting professor in the College of Business at the University of North Texas.

This article looks specifically at the growing trend of "smart buildings" and the cyber issues surrounding the technologies and tools used to create and manage internet-enabled buildings. Due to the rapid increase of Smart Cities and Smart Building technology, commercial real estate companies are having trouble keeping up with the rapid and pervasive changes occurring in building management. It is becoming more difficult to maintain proper policies and procedures for data management and sound data governance practices.

From smart cities to BIM's (Building Information Modeling) to third parties to telecommuting, there are no more islands in our commercial real estate world. There are dangerous entry points everywhere. Integration is becoming the norm and the ability to manage data within this integrated ecosystem has never been more important. Throughout this article we provide a series of questions to help you begin the process of verifying that your building/space is capable of protecting tenants (and you) from data theft.

SMART CITIES

A smart city is an urban area that uses different types of electronic data collection sensors to supply information which is used to manage assets and resources efficiently. This includes data collected from citizens, devices, and assets that are processed and analyzed to monitor and manage traffic and transportation systems, power plants, water supply networks, waste management, law enforcement, information systems, parking, schools, libraries, hospitals, and other community services.[1]

The smart city concept integrates information and communication technology (ICT), and various physical devices connected to the network (the Internet of things or IoT) to optimize the efficiency of city operations and services and connect to citizens.[2,3] Smart city technology enables better decisions in governance, design, and implementation/operation.

As a result of the smart city evolution, cities are becoming huge data centers. A great example of this is a Geographic Information System (GIS). GIS has been used by cities for many years now for more informed decision-making. Cities are realizing that their dispatch centers, sensors, meters, detectors, and traffic controls generate a lot of data which can be mined to better understand how buildings, streets and other assets can be used, optimized, and made safer. As this usage expands, cities must protect the data from inappropriate access (think a driver changing a traffic light so they don't have to stop), and do triage to decide which data to analyze and use.

Likewise, as cities are collecting data on public and privately owned buildings, owners must be aware of what data the city is collecting on their buildings and how that data is being protected and used. In turn, tenants must be aware of what data the landlord collects, can collect, or is being required to collect, by the city. As we will see below, clauses to that effect should be incorporated in commercial leases.

SMART BUILDINGS

Smart buildings are defined as structures in which automated processes and devices are used to control and monitor building operations. As these systems are implemented and ultimately integrated electronically (moving from a "dumb" building to a "smart" building) opportunities are created for increased efficiencies. These systems, when connected to the internet without appropriate security features, are what lead to increased risks of cyberattacks.

Early Building Information Modeling systems (BIMs) allowed building professionals (architects, engineers, builders, consultants etc.) to work from the same model and digital platform. As BIMs evolved to be more sophisticated, they collected working, walking, and daily practice user patterns, enabling interior spaces to better adapt to end-users needs and practices. This enhanced the user's comfort and productivity and resulted in more flexible spaces. As the internet expanded, Building Automated Control Systems (BACs) were integrated into the overall BIM approach. As each new system was integrated into the overall

Table 1 : Vulnerabilities by Property Type

Systems Involved	Owner/ Tenant	Owner/ Tenant	Owner	Owner/ Tenant	Owner/ Tenant	Owner
Entry Points by Property Type	**Mobile/Web Applications**	**Online Payments/Point of Sale (POS)**	**Industrial Control Systems/HVAC/ BMS**	**Employee Devices**	**Webserver/ Network/ Cloud**	**Open Wi-Fi Access**
Hotel	◐	●	◐	●	◐	●
Retail	◐	●	●	◐	◐	●
Health Care	◐	○	●	○	●	○
Multifamily	◐	◐	○	◐	●	◐
Data Center	◐	○	●	○	●	○
Office	○	○	◐	◐	◐	○
Industrial	○	○	◐	○	◐	○

● High ◐ Medium ○ Low

Note: High to low is defined by the level of risk exposure for each property type by each entry point.

Source: Evolving cyber-risk in Commercial real estate, p.4. Deloitte Center for Financial Services analysis

building management system, the opportunities for cyberattacks multiplied. Today the entry points for a cyberattack have expanded.

Table 1 from the Deloitte study on "Evolving Cyber-Risk in Commercial Real Estate"[4] shows that while all property owners and tenants have some degree of exposure to cyberattack, hotel and retail property types are relatively more vulnerable (horizontal blue dotted lines in Table 1). Additionally, data centers are one of the more vulnerable property types in this category due to their network connections and the servers they manage. Web servers, networks, and cloud create entry points on both tenants and landlords systems (vertical blue dotted lines in Table 1). Open guest Wi-Fi access are particularly easy targets. Knowing where a building is vulnerable is the first step in creating an appropriate defense and response plan.

The Deloitte study explains very well how, at the corporate level, the "…growing use of web-based transactions with tenants and vendors, use of cloud services, use of smartphones and tablets under bring your own device (BYOD) policy, and social media presence create multiple access points for the personal data stored by [commercial real estate] companies…";[5] and how, at the asset level, "…the interconnectedness through internet protocol-based networks, HVAC and other industrial control systems, and open Wi-Fi networks increase data vulnerability…"[6]

However, users and clients typically do not ask cybersecurity questions on the construction/rehabilitation/tenant improvements deliverables – still considering them to be a design and facility management exercise more concerned about where partitions and electric outlets are placed, rather than how a system can be hacked. **Table 2** provides a representative sample of key questions that should be asked in every commercial lease.

The more developers and owners add technology and IoT to manage their buildings, the higher the risk of making their structures less flexible to tenants' business needs. This occurs because the owner/tenant technologies compete with each other via conflicting technologies or bandwidth protocols. This conflict creates even more vulnerability points, leading to less-secure buildings and more access to sensitive data.

UPDATED DUE DILIGENCE

The increased use of Building Management Systems (BMS) and intelligent buildings is adding layers of complexity in the commercial real estate business and changing owner-tenant dynamics. Owners' IT systems are more and more connected with their tenants systems, creating new reciprocal vulnerabilities as they become each other's third party risk.

Office buildings typically market and document in their leases physical security whether through the presence of a security desk or doorman, or ID cards or key fobs containing personal information, hours of operations, video surveillance in parking lots etc. However, secure IT infrastructure is not yet considered part of the amenity package.

Similarly, cybersecurity questions ought to be part of acquisition and investment due diligence and contracts. Property Condition Assessment (PCA) reports continue to follow checklists for HVAC and other electrical, plumbing and mechanical systems by type, capacity, condition, defaults and cost to cure. Beyond the physical condition and soundness characteristics, they do not raise awareness of the cyber hygiene of those building systems. The same questions you ask when signing a lease, you should ask in your property acquisition.

Table 2: Cyber Questions to Consider in a Lease

- What are the security controls and maintenance over:
  - Lighting
  - HVAC
  - Building/garage security and access (badges, FOBs…)
  - Shared building internet connectivity
  - Building Wi-Fi networks
  - Building lobby directory kiosks
- Which machines and usual practices are controlled by computers?
- Are there other IoT in the building our own premises have access to?
- What due diligence do you do to secure the systems of your 3rd Party Contractors?
- Are there any systems connected to several tenants?
- Can you require a cyber assessment?
- Has the building ever been hacked through its systems?

DEVELOPING A DEFENSE AND RESPONSE (D&R) PLAN

There are several key components in managing a smart building. First, separate the corporate network from the infrastructure network. Doing so will eliminate "cross contamination" should one network be compromised.

Second, increase communication between IT, Facilities Management, Engineering, and business. Each area should be communicating what has connection to the internet and how that connection is being used, managed, and protected.

Finally, ensure that third parties are involved in the reporting, oversight, management, and protection of data access. Everyone who has access to the building's data must be involved in protecting it.

Because many Building Automated Control Systems (BACs) controls and IoT devices are very limited in their configuration capabilities, proper product selection is imperative. During product selection and implementation it is important to consider that some BACs control consoles offer/require two factor authentication (2FA). If possible, avoid systems that only use passwords which are shared among users. Evaluation of the security between BACs management software and the controllers themselves is also required. All vendors must go through security assessment, even non-traditional ones such as mechanical maintenance vendors. It is imperative that BACs vendors meet the security strategy of your organization. This is best done by including Information Security management and not relying solely on IT operations. As part of this process encourage the BACs developer and installer to suggest security configuration and architecture recommendations based off their previous experiences. Compare these suggestions with IT operations directives to determine the ultimate configuration of the systems.

Table 3: How to Build a Disaster Recovery Plan

A business continuity plan is proactive and meant to protect the business when normal operations are interrupted.

A disaster recovery plan refers to the ability to restore applications and data, and is typically a subset of a business continuity plan. It should include:

- Communicating the importance of the plan so it is not viewed as a mere compliance checklist
- Identifying key stakeholders internally and externally
- Defining how key stakeholders will be reached and how they stay in communication with one another
- Delineating roles so everyone on the list knows what to do and when
- Designing disaster exercises and practice rehearsals at regular intervals
- Having a communication plan (both internal and external) ready after the incident

RESPONSE AND RECOVERY PLANS

Incident response is how you respond when an incident happens. Since the risk of an attack is no longer a question of if, but when and how bad, preparedness is key. The recent devastating hurricanes have highlighted the need for physical preparedness. But just as cities are planning for more resilience to their power grids, companies need to prepare for cybersecurity resilience. It all starts with a sound data governance plan as was discussed in our previous articles.

In preparing for business continuity and disaster recovery (they are not the same), the assessment and triage of which are the most valuable and/or exposed data and systems come first. Planning – which should be driven by strategic goals – should not be underestimated. As an IT exercise, planning can be an opportunity to ask which data, products, and services do we protect and restore first, and why and how. It can also be used to update and/or discard obsolete policies and procedures, while identifying new ones necessary to protect data in the new ecosystem.

Table 3 provides an initial overview of the key components of a disaster recovery plan. Business practices and expectations have evolved over time: initially recovery addressed physical damage such as flood or fire. Then it added terrorist attacks. Now cybersecurity is a key focus. A 24-hour recovery process, while still good, is no longer the gold standard. Companies must be able to "recover on the fly" in terms of continuous operations, while aggressively stopping and removing the effects of a cyberattack. Exercises and tests should be conducted regularly with clear results that are actionable into quantifiable improvements.

INSURANCE

When it comes to cyber insurance, there are various types of coverage. These include:

- Data privacy
- Breach or loss of data
- Regulatory fines and penalties for data breaches
- Cyber extortion
- Business interruption
- Claims from third parties
- Physical losses (property and bodily damages)

Currently, insurance companies are not specifically addressing smart building technologies in their evaluations. The focus is more on traditional IT and Security Operations functions. In talking with various insurance companies, it is not clear whether a claim would be paid out if the breach originated from a controller or IoT device. It might be, but it might not be. To be sure, you should have scenario conversations with your broker to understand what is covered and what is not.

Unlike property or general liability policies which are fairly standardized, prices and exclusions of cyber policies vary widely. Cyber insurance applications used to be very specific but recently, as insurers came to the conclusion that technology changes too rapidly to keep the applications accurate, and courts have rendered inconsistent verdicts, the industry has made a change in philosophy and clauses are getting more generic.

The good news is that if you adopt best security practices and develop a robust and current disaster recovery plan, your insurance premium is likely to be minimized.

Table 4: Cyber Insurance Questions

To the insurance company:

- What are the exclusions: usual ones are product design, software, and reputation losses; are there others?
- Are phishing attacks covered? Courts have rendered conflicting verdicts.

As you fill out the questionnaire:

- What is your preference for network and information security liability, communications and media liability, and regulatory defense expenses?
- Do you have a formal program in place to test or audit network security controls?
- Do you send or accept financial transactions intended for deposit, via the use of remote deposit capture technology (RDC)?

When filling out the questionnaire for cybersecurity insurance, pay careful attention to the wording of the questions. If a question asks if you have certain documents and/or procedures in place, make sure to include those documents and procedures with the questionnaire. Many companies have purchased cyber insurance only to find out that the policy did not pay because the policies and procedures listed in the questionnaire did not exist, were not updated, or were not followed. **Table 4** lists questions that should be asked of the insurance company providing the cyber coverage and your team completing the questionnaire. While not inclusive of all questions, these provide a key starting point to ensure that your cyberattack will be covered.

CONCLUSION

As discussed in the previous two articles in this series, cyber risk is a strategic issue for any business, no matter the size. It begins with the board of directors and should permeate throughout the organization. The need for adequate policies and procedures, staff training, data governance, and adequate budget cannot be overemphasized.

Beyond the data collection issues, connectivity is becoming a new analytical factor for some investors. These investors are exploring smart cities opportunities and are seeking new metrics beyond the classic supply and demand approach in order to future-proof their investments.[7] With more and more data being collected and utilized by smart cities, we must now recognize and incorporate various partners in protecting the assets (physical and digital).

Viewing cybersecurity risks as investment risks factors, the SEC signaled it was an issue not only for companies and their customers or trade partners, but also for their investors. The SEC started issuing cybersecurity disclosures guidelines in 2011 and reinforced them in February 2018.[8] In the 2018 release, the SEC stressed the need for up-to-date policies and procedures, and expanding the disclosure requirement to address how board of directors oversee the management of cybersecurity.

Becoming cyber safe is a partnership with the city, the utility companies, building maintenance firms, owners, tenants, investors, and anyone else who interacts digitally with the assets. Smart, well managed buildings bring added value both to the end-users and the owners/investors. These smart buildings should also balance business and security needs. With too little focus on business, the risk of cyberattack skyrockets. Too much focus on security may restrict a company's ability to get work done.

In these three articles we have attempted to raise awareness of cybersecurity issues related to commercial real estate business. The first article discussed the value of data as a corporate resource and how processes and procedures need to be put in place to protect it. The second article explained how data governance has become a critical issue, why a data life cycles needs to be defined, should be everyone's concern, and explored how data should be handled and protected. This third article addressed key questions around commercial smart buildings and the growing trend of integrating these into smart city ecosystems. In each of the boxes in this article we have provided a limited set of questions that are part of the diagnostic tools we use to assess the cyber readiness of buildings. If you can answer and provide documentation for each of these questions, you have a good start on practicing commercial real estate in the age of smart buildings. •

ENDNOTES

1. McLaren, Duncan; Agyeman, Julian (2015). *Sharing Cities: A Case for Truly Smart and Sustainable Cities*. MIT Press. ISBN 9780262029728.

2. Cohen, Boyd. "The 3 Generations of Smart Cities: Inside the development of the technology driven city". Fast Company website https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities. Posted 8/10/2015. Viewed 9/19/2018.

3. Peris-Ortiz, Marta; Bennett, Dag R.; Yábar, Diana Pérez-Bustamante (2016). *Sustainable Smart Cities: Creating Spaces for Technological, Social and Business Development.* Springer. ISBN 9783319408958.

4. "Evolving cyber risk in commercial real estate: What you don't know can hurt you." Deloitte Center for Financial Services. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-real-estate-evolving-cyber-risk-re-predictions.pdf. 2015 Deloitte Development LLC.

5. "Rising cyber risk in real estate through the rise of smart buildings." Real Estate Predictions 2017. Deloitte Website. https://www2.deloitte.com/nl/nl/pages/real-estate/articles/rising-cyber-risk-in-real-estate-through-the-rise-of-smart-buildings.html. Accessed 10/12/2018.

6. "Evolving cyber risk in commercial real estate: What you don't know can hurt you." Deloitte Center for Financial Services. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-real-estate-evolving-cyber-risk-re-predictions.pdf. 2015 Deloitte Development LLC.

7. M&G Real Estate, M&G European Connectivity Rankings Report, June 2017. https://www.mandg.co.uk/institutions/articles/european-urban-connectivity-ranking/-/media/AD9E1C4D3EC34B9980C577A409ABFA95.pdf. Accessed 12/18/2018.

8. https://www.sec.gov/rules/interp/2018/33-10459.pdf

CRE®
THE COUNSELORS
OF REAL ESTATE®

www.cre.org

This article/submission represents the opinions of the authors/contributors and not necessarily those of The Counselors of Real Estate® or its members. The Counselors assumes no responsibility for the opinions expressed/citations and facts used by the contributors to this publication regardless of whether the articles/submissions are signed.

Published by The Counselors of Real Estate, a not-for-profit organization, 430 N. Michigan Ave., Chicago, IL, 60611. Copyright 2019 by The Counselors of Real Estate. All rights reserved. (Published online at cre.org/rei).

The Counselors of Real Estate®, established in 1953, is an international group of high-profile professionals including members of prominent real estate, financial, legal and accounting firms as well as leaders of government and academia who provide expert, objective advice on complex real property situations and land-related matters. Membership is selective, extended by invitation only. The organization's CRE® (Counselor of Real Estate) credential is granted to all members in recognition of superior problem solving ability in various areas of real estate counseling.

REAL ESTATE ISSUES®

Published by THE COUNSELORS OF REAL ESTATE®

Since its launch in 1976, *Real Estate Issues* has been the premier forum in which the world's foremost real estate thought leaders present innovative ideas, novel strategies, and intriguing commentary on all matters relating to real property.

Visit www.cre.org/rei to view the digital archive of *Real Estate Issues* articles.

Subscribe at www.cre.org/subscribe to receive digital or print editions of *Real Estate Issues*.