GET SMART

Noëlle Brisson FRICS, MAI
Co-Founder
CyberReady, LLC

Michael Savoie PhD
Co-Founder
CyberReady, LLC

As buildings become increasingly technologized, especially after the pandemic, cyber-attacks can put entire properties at risk and require a firmwide security approach.

In light of the recent onslaught of cyber-attacks on American businesses, consider the following:

- 60% of attacks come from misconfigured remote access
- Most attacks could be avoided by simple human behavior
- Most breaches are discovered several months after they have happened
- "Beneath the surface" factors comprise over 95% of the financial impact of a breach

As these statistics show, the days of cyber-attacks being an IT issue are gone. Today, cyber is a business risk similar to market, operations, or financial risk, and must be treated that way. However, there are concrete steps a business can take to minimize their cyber risks—especially those posed by smart buildings.

PRACTICING COMMERCIAL REAL ESTATE IN THE AGE OF SMART BUILDINGS

A "smart building" is a building with infrastructure attached to the internet and/or internet of things (IoT) devices embedded in the building, such as utility meters, HVAC systems, elevators, vending machines, and building information management systems (BIMS), to name a few. Smart buildings become targets for hackers and their risk profile increases *(Exhibit 1)*.

EXHIBIT 1: VULNERABILITIES BY PROPERTY TYPE

Source: Deloitte Center for Financial Services

🟩 HIGH 🟨 MEDIUM 🟦 LOW

	OWNER/TENANT				OWNER	
	MOBILE/WEB APPLICATIONS	ONLINE PAYMENTS/ POINT OF SALE	EMPLOYEE DEVICES	SERVER/ NETWORK/ CLOUD	BUILDING CONTROLS/ HVAC/EMS	OPEN WI-FI ACCESS
HOTEL	🟨	🟩	🟩	🟨	🟨	🟩
RETAIL	🟨	🟩	🟨	🟨	🟩	🟩
HEALTH CARE	🟨	🟦	🟦	🟩	🟩	🟦
MULTI-FAMILY	🟨	🟨	🟨	🟩	🟦	🟨
DATA CENTER	🟨	🟦	🟦	🟩	🟩	🟦
OFFICE	🟦	🟦	🟨	🟨	🟨	🟦
INDUSTRIAL	🟦	🟦	🟦	🟨	🟨	🟦

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

THE EXPONENTIAL GROWTH OF IOT

Data is not the only target for modern hackers. Core systems, such as industrial controls and digital supply chains, are being hacked in a dangerous trend to disrupt and destroy. For example, 2021 became known as the year of the supply chain attack. The first and most notable was the SolarWinds supply chain attack identified in early January of that year. "Ransomware-as-a-service" (RaaS) also made headlines in May 2021 when Colonial Pipeline, was hit with an attack using the DarkSide RaaS.

Many IoT devices are out of sight, which, in many cases, means out of mind. Most people are not even aware of how many IoT devices exist within their building and what remote access to equipment for evaluation and repair and connection to municipal grids means. Attacks on IoT devices now make up roughly 33% of infected devices. Connected elevators, smart HVAC meters, printers, coffeemakers, interactive kiosks, and other seemingly innocuous connected devices became a cybercriminal favorite in 2020 and continued to be targeted in 2021.[1]

Cyber criminals are also adapting their attack methods. They are targeting the human layer—the weakest link in cyber defense. According to the Verizon 2022 Data Breach Investigations report, the human element continues to drive breaches. In 2021, 82% of breaches involved a human element.[2]

With the increased frequency of cyber-attacks and a heightened awareness of the need for data privacy, many governing bodies, as well as professional and trade organizations started issuing law, regulations, directives, and guidance notes.

EXPANSION OF LAWS AND REGULATIONS

With the increased frequency of cyber-attacks and a heightened awareness of the need for data privacy, many governing bodies, as well as professional and trade organizations started issuing law, regulations, directives, and guidance notes. Abroad and in the US, a few examples of increased awareness of cyber risks and heightened regulatory scrutiny are worth mentioning.

Government

Decades ago, the US Congress started regulating the use of sensitive "personally identifiable information" (PII). For example, since 1974, the Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. In 1996, the Healthcare Insurance Portability and Accountability Act (HIPAA) addressed the security and privacy of health information.

This concern for sensitive information took a huge leap in 2016 when the European Commission issued the General Data Protection Regulation (GDPR) to protect the data privacy of European citizens. Since GDPR subsequently became enforceable in 2018, many other countries across the globe issued laws modeled after it, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), as well as the UK's version of GDPR.

In the US, similar regulations (albeit for consumers, not citizens) have been adopted at the state level. California was an early adopter of similar regulations when it passed the Consumer Protection Act (CCPA). Similar statutes followed in Connecticut, Colorado, Utah, and Virginia. Several other eastern states are pondering comparable legislation. The Securities and Exchange Commission (SEC) also strengthened its guidance to assist public companies in preparing cyber risks and incidents disclosures: 10K and 10Q filings will need to include more information on the company's risk management procedures. Furthermore, data breaches will need to be reported, including costs and litigations.

The European Energy Performance of Buildings Directive (EPBD) introduced the concept of a Smart Readiness Indicator (SRI) as a common EU scheme for rating the smart readiness of buildings.[3] SRI aims to "raise awareness on the benefits of smarter building technologies and make their added value more tangible for building users, owners, tenants, and smart service providers." Although it focuses on energy saving and well-being, it points to the overriding interrelationships between all smart infrastructure and networks interacting within a building. As those relationships increase, the entry points of a cyber-attack multiply.

Private Sector

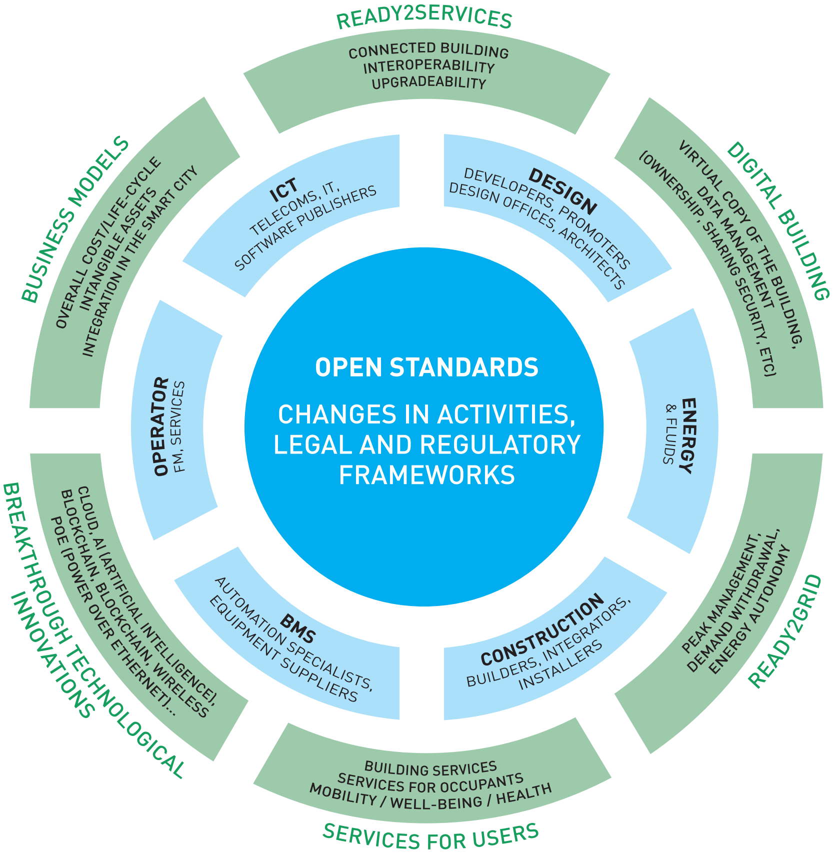
The private sector is also mobilizing to strengthen data protection. On the global stage, the Basel Committee on Banking Supervision in 2021 further raised the importance of sufficient IT risk control measures to minimize that category of operational risks. The International Standards Organization is in the process of updating ISO 27001 and keeps expanding standards dealing with information security and data protection. More recently, the World Economic Forum identified the need to bridge the gap between decision-makers and technical experts, and launched a cybersecurity platform which among other initiatives, is developing a cyber resilience index for businesses.

There are also several examples of data protection particularly relevant to commercial real estate:

- The National Elevator Industry, Inc. (NEII) released *Elevator & Escalator Industry Cybersecurity Best Practices* in 2019, a guideline developed by cybersecurity and codes experts from NEII member companies and international industry partners.
- In the UK, in 2022, the National Cyber Security Centre (NCSC) and the Chartered Institute of Building (CIOB) partnered to help small-to-medium sized construction companies protect their businesses and building projects from cyber-attacks.
- In 2021, the European Association for Investors in Non-Listed Real Estate Vehicles (INREV) implemented ISO 27001 and committed to cybersecurity best practices to better protect their members' data as they revamped their data warehouse.

EXHIBIT 2: THE SMART BUILDING ECOSYSTEM

Source: Smart Buildings Alliance



RAISED AWARENESS OF THE RELATIONSHIP WITH SMART GRIDS AND SMART CITIES

Traditionally, a city was an urban area where people and physical infrastructure interacted. A smart city adds a technology layer and uses different types of electronic data collection sensors to supply information used to manage assets and resources. 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.[4]

Geographic Information Systems (GISs) have also been used by cities for many years now for more informed decision-making. Cities are now developing Digital Twins using this data to better understand how buildings, streets, and other assets can be used, optimized, and made safer.

The increasing deployment of smart city technologies is turning cities and buildings into huge data centers. As interconnection increases, so does the risk of data being used for inappropriate activities. Cities are collecting more and more data on public and privately-owned buildings to be more efficient and meet evolving sustainability requirements. And while smart cities have the potential to be more efficient, they present risks without proper management and oversight of data usage. This explains, for example, the notorious abandonment of the Quayside project by Sidewalk Labs in Toronto over fear of obtrusive data collection.[5]

DATA GOVERNANCE

Despite the recent and emerging data regulations, not enough importance is given to data governance. There is a compelling need to discuss data governance not from a regulatory stance but from a holistic risk approach.

Shared services, IoT, and third parties multiply the opportunities for data being compromised or stolen. It is imperative that organizations define the "right data" so it can be protected. Right data is that needed by the organization to reliably achieve its strategic goals. The problem today is that because it is so easy to collect data, organizations are drowning in data. In fact, too much data may even obscure transparency. For example, the French regulator Autorité des Marchés Financiers (AMF) sees too much data submission as a red flag for risk.[6] By first defining what constitutes its "right" data, an organization can become more selective. This approach not only reduces costs, it speeds-up response times if there is breach.

The second key step is an accurate and up-to-date inventory of business data, categorized by departments and/or risk owners. Through that inventory, companies will know which assets or devices are holding the right data and information. It will be easier then to drive a more relevant risk and resource allocation, and to map those items of risk toward an acceptable and actionable framework. This is particularly relevant in the case of remote workers or bring-your-own-device (BYOD) practices sometimes accepted by companies.

The third step is to organize the data flow to document how the various business lines use the data: why is the data needed in the first place, how end-users process it, and what happens to this data from creation through using, sharing, storing, updating, and finally archiving or deleting it.

The lifecycle of data should be given scrutiny: is there a vetting process for when data comes in and when it leaves your control? Do you know who owns the data? The value chain of data ownership can be very complicated since it often involves aggregation from many sources.

Finally, a set of controls and audit procedures must be in place to ensure ongoing compliance with internal data policies and external government regulations. Data governance should extend to third parties: the same data issues raised and resolved internally should be addressed in interactions with external entities.

A cyber "bonus" is starting to emerge in large cities, with small rental premiums, faster absorption, or better retention, and less downtime between tenants.

UPDATED UNDERWRITING

Appraisers inspections and valuation assumptions do not yet take into full consideration cybersecurity risks, the potential impact on marketability of the building, how "smart" the building is, the level of connectivity, or the presence or absence of cyber clauses in leases. 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. However, beyond the physical condition and soundness characteristics, these reports do not raise awareness of the cyber hygiene of building systems. In that respect, the analysis of obsolescence needs to be expanded.

In their marketing and leases, office buildings typically document 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, and so on. However, a secure IT infrastructure is not yet systematically considered part of this same amenity package.

To meet the growing threat of cyber risk, cybersecurity issues should be included in leases. Any systems connected to several tenants, shared building internet connectivity, interactive lobby directory kiosks, and other shared assets should all be identified, and access documented. Landlords and tenants should conduct cyber sweeps to make sure that previous tenants' accounts have been deleted from hubs, routers, and devices prior to providing access to new occupants.

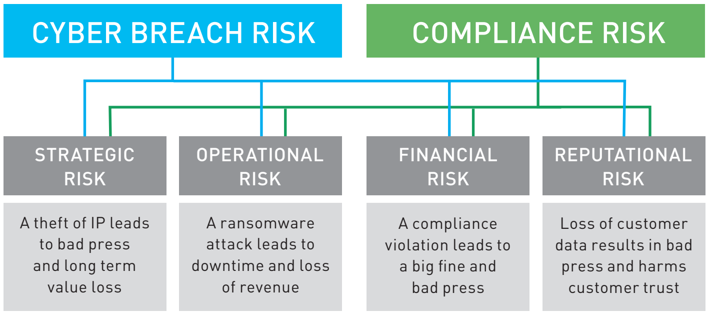
From our experience, a cyber "bonus" is starting to emerge in large cities, with small rental premiums, faster absorption, or better retention, and less downtime between tenants. The valuation industry over the years has developed a framework for "green values." The same thing needs to happen with "cyber values." In the meantime, those issues should become incorporated in acquisition and investment due diligence and contracts.

BUILDING A BUSINESS CASE FOR CYBER RESILIENCE

All steps typically included in due diligence should be updated through a cyber lens. If we agree that cyber issues are an enterprise-wide risk, the analysis should start with a closer look at the organizational chart to detect potential silos and understand how cyber risks are managed. Similarly, routine documents such as contracts, licenses, and permit reviews should make sure that data security is addressed to vet, select, and manage third parties. These are typically the forgotten and weakest elements of a digital ecosystem, because they can be tedious to identify. However, according to IBM's Cost of Data Breach Report 2021, there was a 10% increase in the average total cost of a breach between 2020 and 2021. Where remote work was a factor in causing the breach, there was a cost difference of US$1.07 million.[7]

EXHIBIT 3: EFFECTIVE RESPONSE REQUIRES MANAGING BUSINESS-LEVEL RISK

Source: balbix.com


CYBER BREACH RISK

COMPLIANCE RISK

STRATEGIC RISK

A theft of IP leads to bad press and long term value loss

OPERATIONAL RISK

A ransomware attack leads to downtime and loss of revenue

FINANCIAL RISK

A compliance violation leads to a big fine and bad press

REPUTATIONAL RISK

Loss of customer data results in bad press and harms customer trust

Because more than 90% of hacks involve human error, training programs should also be assessed to check if they include cyber risks and are kept up-to-date and are delivered throughout the company.

Because more than 90% of hacks involve human error, training programs should also be assessed to check if they include cyber risks and are kept up-to-date and are delivered throughout the company. Particular attention should be focused on data governance and business continuity, including disaster recovery plans and protection of customer information. If the target company or building has been hacked, a detailed understanding should emerge from the source and circumstances of the hack to the handling of the crisis and corrective measures taken.

The hacking history of a building should be the parallel to the credit history of a company. The Strengthening American Cybersecurity Act passed by the Senate in March 2022 will establish a mandate for companies in critical sectors (e.g., energy, transportation, financial services, health care, etc.) to alert the government when they are hacked or faced with the demand to pay ransoms to hackers.

Additional representations and warranties should cover data security and address how employees, clients, and third parties' confidential data are protected, whether there have been data breaches, whether asset and property managers procedures are in compliance with the recent laws enacted in many states, and whether systems and networks have been properly configured to protect confidential data.

Similarly, indemnification provisions should require that the target indemnify the buyer for any costs incurred in connection with losses associated with privacy or data security. Coverage should be aligned with the risk map of the company and its real estate assets.

NEW DYNAMICS FOR LANDLORDS, TENANTS, AND PORTFOLIO, ASSET, AND PROPERTY MANAGERS

Everyone who has access to the building's data must be involved in protecting it. Owners, managers, and tenants are becoming third-party risks to each other.

To start with this unified all-user protection, facilities managers need to re-invent themselves as "great facilitators" to increase communication between third parties, IT, Eegineering, and business leaders, understanding their relations and striving to break silos between those stakeholders. Each area should be communicating what has connection to the internet and how that connection is being used, managed, and protected.

On the front-end, property and asset managers and landlords need to have similar conversations with tenants who need to understand how the building operates and will increasingly demand that their buildings include safeguards to protect their data and require proof and accountability in their leases. Conversely, building owners and managers should assess the vulnerability presented by new and existing tenants.

MANAGING FUTURE RISKS

Advancing an effective and holistic response to cybersecurity requires managing business-level risk, rather than just IT-level risk. It is the only way to build effective business continuity and disaster recovery plans.

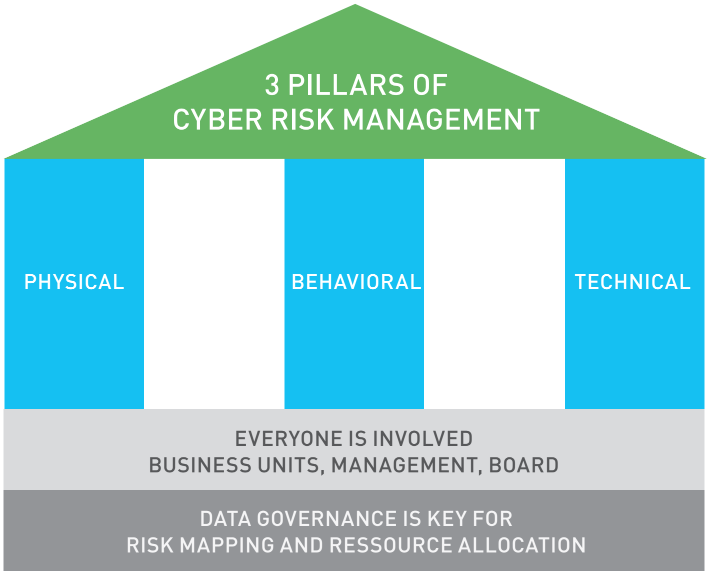
Modern cyber risk management must address:

1. Physical Security: Are buildings and building operations secure from intruders? Is sensitive data protected from prying eyes (these could be intentional, accidental, or even remote through video conferencing)?
2. Behavioral Security: Do personnel understand and practice safe data management practices? Do employees understand how to spot a phishing attack? Are safe protocols followed when entering and exiting spaces containing sensitive data? Is line-of-sight checked when participating in a video call?
3. Technical Security: Is the network secure? This seems a simple question, but with the addition of remote workers, IoT devices, and cloud storage, the network is no longer limited to the office. Technical security must focus on protecting the data wherever it is flowing.

Finally, it is not enough to protect each of these areas. Good cyber risk management must address the interaction between them. For instance, increasing password security may tighten technical security, but if the passwords are too complex, users will write them down and/or store them on unprotected smart phones, resulting in decreased behavioral security, and, possibly, an overall decrease in the cyber risk profile of the organization.

Now more than ever organizations need to treat cyber risk as a business risk. Whether it is a smart building, interconnected devices, or remote workers accessing an office network with personal devices, private data is more accessible, and more vulnerable to attack.

It is possible to manage the cyber environment and proactively protect sensitive information. Just start the process. Doing so will open new conversations with tenants, investors, and trade professionals, and create a more competitive building and portfolio.


3 PILLARS OF
CYBER RISK MANAGEMENT
PHYSICAL
BEHAVIORAL
TECHNICAL
EVERYONE IS INVOLVED
BUSINESS UNITS, MANAGEMENT, BOARD
DATA GOVERNANCE IS KEY FOR
RISK MAPPING AND RESSOURCE ALLOCATION

ABOUT THE AUTHORS

Noëlle Brisson, FRICS, MAI, and Michael Savoie, PhD, are Co-Founders of CyberReady, LLC, which provides cyber risk management, and state-of-the-art online and in-person assessments of the cyber risk profile of an organization's physical, behavioral and technical assets.

NOTES

[1] Nokia Threat Intelligence Report 2021. onestore.nokia.com/asset/210870. Accessed 6/27/2022.

[2] 2022 Data Breach Investigation Report (DBIR) | Verizon. (verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf). Accessed 6/27/2022.

[3] “Smart Readiness Indicator—Smartbuilt4eu”. smartbuilt4eu.eu/. Accessed 6/28/2022.

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

[5] (triplepundit.com/story/2020/sidewalk-labs-failure-smart-cities/120616). Accessed 6/26/2022.

[6] Brisson, Marie-Noelle, Savoie, Michael. “Data Governance: Cybersecurity Oversight and Strategy for Real Estate.” Real Estate Issues, Volume 42:10. August 28, 2018.

[7] Cost of a Data Breach Report 2021; ibm.com/downloads/cas/OJDVQGRY. Accessed 6/27/2022.

The increasing deployment of smart city technologies is turning cities and buildings into huge data centers. As interconnection increases, so does the risk of data being used for inappropriate activities.