



Grant Thornton

An instinct for growth™

The hidden cost of smart buildings

Understanding cyber risk for asset managers and owners

Updated November 2019



Asset management issues for boards

Across the world, tenants have increasing expectations of intelligent buildings providing them access to technology and automated systems—from online storage to health and safety, communications, climate control, lighting, security and more.

The market for smart buildings in the Americas is expected to reach US \$8.84 billion by 2021.¹ As an asset owner, huge gains can come from the automation and optimization of services and increasing the sustainability rating of the asset.

Despite adding value, the increased connectivity of these smart services can have a negative side. They can expose those who occupy them to a higher risk of cyber attack through “disruption of service” or potential gateways to data. For building owners and operators, it’s a classic trade-off between value and risk. Any investments in smart buildings and services needs to include the appropriate consideration of cybersecurity.

The threat exists for all asset classes across the real estate industry: **office and apartment blocks, data centres, industrial sites, and even public spaces like hospitals, universities, hotels and shopping centres.**

In 2016, an “ethical” hacker highlighted the threat to smart buildings by tapping into the network of a highly automated five-star hotel in China. By taking control of many of the rooms, he was able to demonstrate just what can occur if controls are not stringent enough.²

Cyber risk management and data protection need to be key elements of the investment in smart buildings at all stages of the asset lifecycle. Securing your asset against cyber attacks is about ensuring your ability to get the right return on your investment in a smart building.

1. <http://www.businesswire.com/news/home/20170621006367/en/Global-Smart-Buildings-Market-Boost-Increasing-Demand>
2. <http://www.scmp.com/news/china/article/1561458/hacker-takes-control-hundreds-rooms-hi-tech-shenzhen-hotel>

Smart building cyber risk is everyone's risk

As we describe in our recent Grant Thornton International report [“Locking down the value of data,”](#) one of the biggest challenges facing today's leaders is ensuring that their businesses can anticipate and mitigate cyber risk. For the asset manager or owner, a cyber attack on a building could have a significant impact on reputation and operations. The issue of cybersecurity should sit squarely on the boardroom table of building owners and management companies.

While accessing building systems may not appear to be a high-impact risk, it does provide a gateway to higher-value assets attached to or stored within, such as sensitive tenant data. In addition, the increase in automated systems allows cyber attacks to become more “physical” through the cutting of services, access or safety and security systems—putting occupants' safety at risk.

In 2013, retail group Target fell victim to a cyber attack when hackers gained access to customer data records via the company that supplied their heating and air conditioning system.³ The company's breach resulted in a litigation bill that has so far reached almost US \$300 million—and that doesn't include the harm to the organization's reputation and revenues, which is much harder to measure.⁴ The repercussions of this particular attack are ongoing.

More recently, the infamous WannaCry worldwide ransomware attack in May 2017 targeted computers running Microsoft Windows operating systems, affecting thousands of organizations and businesses in 150 countries, including the NHS⁵ in the United Kingdom. Such a large-scale attack shows how vulnerable the software that drives the connectivity and systems in our smart buildings can be, and reiterates the need for advanced security systems and firewalls in our smart buildings.

“The increased convenience of smart buildings does come with new risks—risks that are not yet fully understood by owners and occupiers.”

Joy Shuchat, Partner, Real Estate & Construction

If a building shuts down due to its security and systems being compromised—whether it be exposure of tenant data, break down of power supply, or restricting access to the building—the reputational damage could put the continuity of the asset owner's organization at risk.

Given the potential reputational and financial penalties of getting it wrong, cyber resilience begins with the C-suite and should engage a range of internal and external stakeholders. The pervasiveness of technology in all organizations means managing technology risk is no longer just the responsibility of the IT department.

3. <https://www.dlapiper.com/en/us/insights/publications/2017/05/smart-buildings-not-all-just-bricks-and-mortar/>

4. <http://www.businessinsurance.com/article/20160718/NEWS06/160719794/target-data-breach-2013-lawsuit->

5. <https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20>



Seeking chinks in the data armour

Hackers are constantly looking for the points of least resistance that give them access to, or control over, an organization's data and systems. Often, that point of least resistance is in the supply chain, which could include the owners or managers of the buildings, where they operate or store their assets.

Naturally, tenants expect to be secure. They have a right to assume that you, as the owner or building manager, have done everything possible to make their building resilient and resistant to attack, and will not open up their own business to risk.

It's too cost-prohibitive to mitigate all risk. Every organization can be a target, whether it be the profile of your tenants or the nature of the asset that attracts attention. Inevitably, some attacks will succeed. Those who carry out the attacks are constantly perfecting their skills and testing the boundaries of what they can access. It's those with malicious intent that we need to be ready for.

Real estate assets will always be a mix of the old and the new. While it's more cost-effective to incorporate cybersecurity from the design phase, this isn't always possible. Any retrofit solutions or upgrades to automate older assets need to make sure that cyber risk has been considered and mitigated to the extent possible.

“Real estate businesses must ask themselves: ‘As property owners, are we using due diligence properly to prevent our building’s systems from being a point of entry for hackers into larger organizations?’”

Mohamed Elghazouly, Senior Manager, Cybersecurity

Cyber resilience and real estate

Taking a pragmatic and realistic approach to cybersecurity, understanding the current and future risks, and quantifying what it would mean to your business and your tenants, makes it easier to formulate data and security protocols. You can then build a resilient business with contingency plans that help you withstand and recover from a crisis, while maximizing the return on your smart building investment.

There are no holistic solutions for cybersecurity, but the best-protected companies have, as a bare minimum, a set of disciplines and policies in place that gives them the essential framework for an attack-resistant organization. Critically, these are owned at board level. This is as true of a real estate or construction business as it is in any other industry.

“As building software and accounting systems move towards more cloud solutions and integrated systems, these will create a range of cyber threats.”

John Di Liso, Partner
National leader, Real Estate & Construction

Everything any organization does to protect itself can be quickly unravelled if an employee unknowingly clicks on a malicious link. A moment of distraction can have huge consequences, not just to the business, but also of its tenants and their staff. This highlights the importance of appropriate cyber training and awareness throughout the organization.



How can you best protect your business?

We recommend the following:

- **Identify** and understand your organization's assets: people, premises, products, processes, IP, information and brand.
- **Test** the cyber and physical vulnerabilities of each asset, and establish which threats are most prevalent—both now and in the future.
- **Employ** controls that restrict your employees, suppliers and the public to only the information that they actually need.
- **Segregate** tenant and landlord networks where practical.
- **Securely** back-up all essential data, and regularly test it.
- **Instill** a robust and effective recovery strategy that enables the fastest possible return to normality.
- **Ensure** those in your supply chain are aware of their cybersecurity responsibility, and validate that they are meeting your expectations.
- **Set, communicate, embed and test** employee behaviours that protect your business assets and your reputation.

Improving your resistance to attack

Our cybersecurity and real estate and construction teams work together to create bespoke security programs for companies at all levels of the industry.

It's by combining our understanding of the issues you face every day with the data security expertise of our cyber specialists that we can best increase your resilience.

We leave as little as possible to chance. For example, we can evaluate your current security position, create a bespoke program that ranges from security awareness training and testing, to forensic analysis and creating policies, standards and processes.

To find out more about our cybersecurity services for real estate and construction companies, or how you could improve cyber resilience for your business, [contact us](#).



GrantThornton.ca

Audit | Tax | Advisory

© 2019 Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd. All rights reserved.

About Grant Thornton in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide. A listing of Grant Thornton offices and contact information can be found at: www.GrantThornton.ca