Grant Thornton

An instinct for growth™

Real estate

Cyber security

Risk

The hidden cost of smart buildings

Understanding cyber risk for asset managers and owners

October 2017

Contents

Section	Page
Asset management issues for boards	01
Smart building cyber risk is everyone's risk	02
Cyber resilience and real estate	04
Improving your resistance to attack	05

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.

As an example, around 20% of the UK's commercial buildings are defined as 'smart', and the world's smart building market is expected to be worth up to $24.73 billion by 2021[1]. As an asset owner, huge gains can come from the automation and optimisation 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 open up 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 cyber security.

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.

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.

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].

1. https://www.jltspecialty.com/our-insights/thought-leadership/real-estate/new-cyber-risks-and-liabilities-for-property-owners-in-2017
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 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. As an asset manager or owner, while the risk is primarily with your tenants, if an attack occurs the impact on the building's reputation and your own could be devastating. Therefore, the issue of cyber security 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 became victim of 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 failing in their due diligence resulted in a litigation bill that has so far reached $500 million – and that doesn't include the harm to the organisation's reputation and revenues which is much harder to measure. The repercussions of this particular attack are therefore ongoing.

More recently, the infamous WannaCry worldwide ransomware attack in May 2017 targeted computers running Microsoft Windows operating systems, affecting thousands of organisations and businesses in 150 countries, including the NHS[4] in the UK. 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"
>
> **Kersten Muller, 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 organisation 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 organisations has meant 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. 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 organisation'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 suppose 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 organisation can be a target, whether it be the profile of your tenants or the nature of the asset that attracts attention, but 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 cyber security 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 being a point of entry for hackers into larger organisations?"
>
> **Sunil G. Chand, Director, Cybersecurity**

Cyber resilience and real estate

By taking a pragmatic and realistic approach to cyber security, 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 maximising the return on your smart building investment.

There are no holistic solutions for cyber security, 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 organisation. 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.

"Smart buildings face increasing vulnerability – the higher levels of connectivity and integrated control systems open them up to a range of cyber threats."

Sian Sinclair
Global industry leader - real estate & construction

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

How can you best protect your business?

We recommend the following:

- Identify and understand your organisation'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
- Instil a robust and effective recovery strategy that enables the fastest possible return to normality
- Ensure those in your supply chain are aware of their cyber security 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 global cyber security and real estate and construction teams work together to create bespoke security programmes 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 programme that ranges from security awareness training and testing, to forensic analysis and creating policies, standards and processes.

Contact us

To find out more about our cyber security services for real estate and construction companies, or how you could improve cyber resilience for your business, contact one of our member firm specialists:

Grant Thornton Australia

Sian Sinclair
Global industry leader – real estate & construction
sian.sinclair@au.gt.com

Grant Thornton Canada

Sunil G. Chand
Director, cyber specialist
sunil.chand@ca.gt.com

Bo Mocherniak
Partner, RE&C specialist
bo.mocherniak@ca.gt.com

Grant Thornton China

Wilfred Chiu
Partner, RE&C specialist
wilfred.chiu@cn.gt.com

Grant Thornton Ireland

Mike Harris
Partner, cyber specialist
mike.harris@ie.gt.com

Grant Thornton Netherlands

Mark Hoekstra
Partner, cyber specialist
mark.hoekstra@gt.nl

Grant Thornton UK

Kersten Muller
Partner, RE&C specialist
kersten.j.muller@uk.gt.com

Manu Sharma
Director, cyber specialist
manu.sharma@uk.gt.com

Grant Thornton US

Vishal Chawla
Partner, cyber specialist
vishal.chawla@us.gt.com

Greg Ross
Partner, RE&C specialist
greg.ross@us.gt.com

Grant Thornton
An instinct for growth™

grantthornton.global

EPI.169