ANREV

Cybersecurity – Securing real estate assets in a digital age

Introduction

Real estate professionals have traditionally focused their attention on the physical aspects of security, safeguarding their properties from damage, intruders and natural disasters. However, with real estate businesses becoming more reliant on data, connectivity and other digital technologies, they are now also open to cybersecurity threats. Indeed, recent high-profile attacks have shown the ways in which the sector is vulnerable to security breaches through everyday systems such as lighting, access control and air-conditioning. Cybersecurity threats are changing the way real estate professionals approach asset management, and this is becoming a leading factor in decision making processes.

What is cybersecurity?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from any unauthorised use or access. In the context of the real estate sector, it represents the ability of systems to defend against cyber intrusions and recover from incidents such as hard drive failures or power outages and withstand attacks from adversaries such as hackers and criminal organisations.

How is it relevant to real estate?

Cyber-attackers have specifically targeted real estate businesses in a string of breaches in the past few years. In 2013, hackers used security credentials stolen from a heating, ventilation and air-conditioning (HVAC) operator to gain access to the credit and debit card records of Target's customers. The HVAC operator in the Target data breach is not the first real estate company – nor would it be the last – to fall victim to a cyber-attack. There are several reasons why the real estate sector is an attractive target for hackers:

- **Interconnected devices** – Apartment, retail and office assets are becoming "smarter". They are connected to other devices via the Internet, creating potential avenues for hackers to utilise connected technologies like smart locks and lights, environmental controls and voice-assisted devices to gain access to those assets. Recent examples include hotel guests being locked out of their rooms by a hacker manipulating digital locks remotely.

- **Valuable digital assets** – Real estate businesses store lease agreements, rental applications, credit reports and deal financing terms in their computer systems, all of which are filled with payments information and the confidential and often personal data of tenants and clients.

- **High-profile tenants** – Owners of properties with high-profile tenants, such as banks, departmental stores or fashion retailers, may be targets of cyber-attacks intended ultimately to steal confidential or financial information from those tenants.

- **High-value transfers** – Real estate businesses often transfer huge sums of money online and they could be targeted for the cash from such transfers.

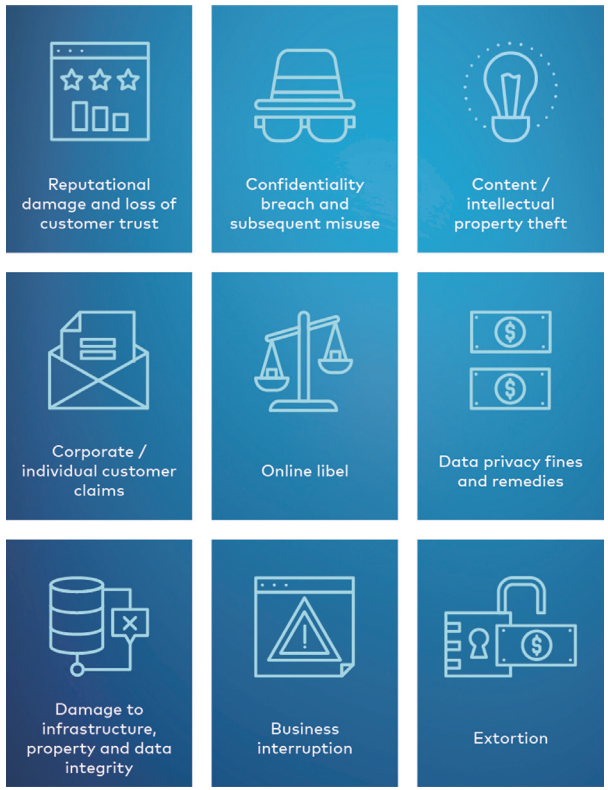
- **Third party infrastructure and services** – Real estate companies often leverage third-party infrastructure and services to support their operations. Without the right safeguards (such as security due diligence and contractual protections) in place, the company would be at risk of suffering a cyber-attack, as a vulnerability in a service provider's cybersecurity could leave the entire network exposed to the hacker.

- **Lack of regulation** – the institutional real estate sector is subject to far less onerous regulation compare to other sectors such as financial institutions and telecommunications. As a result, there is less onus and therefore less investment in implementing information and system security programs, leaving such information and systems more vulnerable to attack.

What are the risks?

Risks associated with cyber-attacks range from the obvious – loss and corruption of data and confidentiality breaches – to the less obvious but potentially even more damaging – regulatory fines and reputational damage. It is also increasingly obvious that cyber-attacks threaten both operational and physical systems – each with the potential to disrupt Business-as-Usual across the full real estate spectrum, from retail to healthcare and office to logistics.

Figure 1: Cybersecurity risks



What are the common threats?

Cyber-attacks against real estate businesses are evolving all the time but common patterns and strategies have emerged.

Figure 2: Common attack types and potential assailants

Common attack types
- Malware distribution
- Ransomware
- Distributed denial-of-service (DDOS) attacks
- Compromising privileged accounts

Common attackers
- Cyber criminals
- Terrorist groups
- Hackers
- Disgruntled employees or contractors
- Competitors in the real estate industry

What should real estate professionals do next?

Cybersecurity should be viewed as more than a technological risk. It should be approached as a core pillar of a real estate company's business strategy and must begin with the company identifying the key networked assets and the associated cybersecurity risks. Once identified, the company must then complete a series of steps to understand where they are and where they need to go next (Figure 3).

Figure 3: Cybersecurity roadmap

Step 1: Consider the key networked assets and threat/risks.

Step 2: Understand your legal, regulatory and contractual obligations.
- Understand the legal and regulatory obligations your company is subject to (e.g. obligation to notify regulators or customers within a specified time period if a data breach occurs).
- Understand the contractual security obligations your company may be subject to and be proactive in negotiating more robust information security provisions in your service contracts for everything from building maintenance to cloud computing.

Step 3: Build your cybersecurity strategy.
- Build a "benchmark standard" (based on the legal, regulatory and contractual obligations identified in step 2) against which you will measure your company's cybersecurity practice.
- Carry out an audit of your company's cybersecurity practices and determine where it is falling short of the required standards.
- Develop and implement a rectification plan to address any weaknesses.
- Communicate the cybersecurity strategy with the rest of the business and conduct regular training across the whole workforce, e.g. cybersecurity training as part of mandated compliance training.

- Keep the cybersecurity strategy under constant review to ensure that it addresses the latest threats as well as the latest legal and regulatory changes impacting your company.

Step 4: Implement an incident response procedure.

- Have in place a procedure to respond to cybersecurity incidents.
- Test the incident response procedure regularly to ensure that it is fit for purpose and that each relevant team member knows what is required of them.
- If a breach occurs, ensure that your company follows the steps listed out in the incident response plan.

Step 5: Manage third parties.

- Be aware of your partners' security standards and track record in cybersecurity.
- Ensure that your partners give you control and visibility over your data and content, and are transparent about where they store data and content.
- Ensure that your partners have a suitable business continuity plan in the event of data breach.
- Have in place appropriate limitations restricting the situations in which your partners can sub-contract or share your data and content.
- Have a robust contract in place with your partners capturing all of the necessary security and confidentiality requirements.

If members have any questions, or require a more detailed explanation of any of the points referenced in this note, please contact the ANREV Technology and Innovation Working Group at the following e-mail address: wg-tech-and-innov@anrev.org

We would also be keen to hear members' experiences on cybersecurity, and/or their views on how the industry's cybersecurity best practices will evolve in the coming years.