Deloitte.

Real estate cyber security
Securing the future of sustainable smart buildings

MAKING AN IMPACT THAT MATTERS since 1845

Traditionally, real estate is about bricks and mortar, but its future lies in advanced analytics and improved user experience. Sensors and servos will collect and deploy data intelligently, as the lifeblood of smart, efficient buildings that respond to users' needs. This convergence of innovation and infrastructure will enable the jobs of the future, underpin economic prosperity, and drive the move to greater sustainability.

Technologies such as water conservation, HVAC optimisation, solar panels and other renewable sources can transform the environmental impact of buildings, while building automation systems and predictive maintenance can streamline their management. This minimises wasted time, materials, costs and energy. Buildings currently represent 40% of global energy consumption and 33% of all greenhouse gas emissions, so smart buildings will give the real estate sector a leading role in shaping a sustainable future.[1]

Data-driven benefits...

This opportunity to shape the future is huge, and will depend on equipping buildings with connected devices. Operationally, connected firewalls can reduce response times in emergency situations, motion sensors can help manage heating and lighting to save energy, while digital access controls can tailor access to spaces and thoroughfares for different individuals.

Data from such devices can also provide behavioural insights for building management, but must be used effectively and ethically, to maximise its benefits while respecting individual privacy.

For instance, patterns in the data might reveal that an employee commutes a short distance by car instead of walking, which might prompt the building manager to consider the reasons for such behaviour. These insights can then inform human solutions, such as an employee shuttle bus or working patterns that avoid walking alone at night, to promote both sustainability and employee wellbeing. Smart buildings can provide the data that helps organisations ask smart questions and work better.

...but exposure to risk

The big emerging threat, though, is a cyber-attack, which is gaining prominence in many portfolios' risk registers. Such cyber-attacks could have a severe commercial impact on businesses that rely on digitalisation to meet performance targets, and cannot afford to lose any uptime.

[1] Why buildings are the foundation of an energy-efficient future, World Economic Forum, February 2021.

Unlike traditional buildings, the fabric of smart buildings – with many interconnected devices – presents a large attack surface, which must be secured. Legacy systems might have been designed for a less connected age, digital products might be insecure, and the wide variety of devices, vendors and standards could lead to major vulnerabilities. Internet of Things (IoT) devices, for instance, often lack secure protocols or consistent standards, making it hard to be certain that a smart building is also a secure building. Meanwhile, at national level, there are growing security concerns that some vendors' devices could be vehicles for hostile powers.

Bad actors might include nation states, disgruntled ex-employees or organised crime, and attacks are already a reality. Building managers have lost control when automation systems have been hijacked, hacked HVAC systems have jeopardised the safety of hospitals, and thousands of solar panel stations have been found to have security vulnerabilities. Meanwhile, shopping centres, hotels and parking garages – particularly those that have embraced digital transformation – can be susceptible to a range of cyber-attacks, and make attractive targets for cyber criminals, due to their essential function in society.

Environmental considerations

While such attacks can do commercial or reputational damage to the organisations concerned, they can have a wider impact on global sustainability. Not only do they undermine the environmental benefits of building management technologies, but they also spread fear and slow the adoption of sustainable solutions.

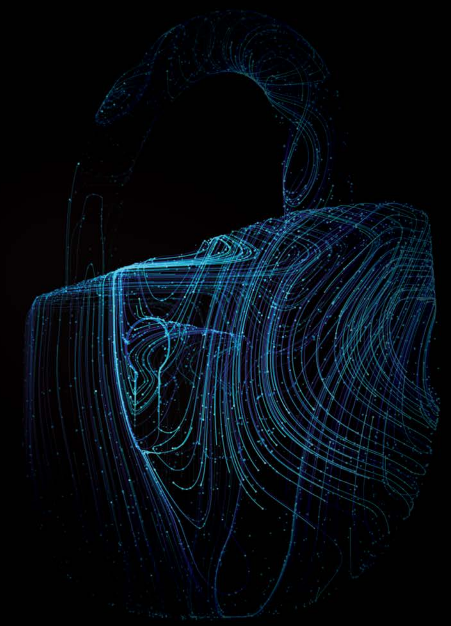
The good news is that such risks can be mitigated. The technology, and associated risks, might be new in real estate, but they are well-known in other sectors. New threats are constantly emerging, but the art of staying watchful is well-developed. Such vigilance does, however, require the existence of threats to be acknowledged, and many real estate companies have not yet woken up to their reality.

Effective security

Once the challenge is acknowledged, cyber risk real estate experts can advise on the most effective way to move building management systems and other estate technologies from their current state to a state in which cybersecurity is managed. At the heart of this approach is a clear understanding of each organisation's particular business, critical priorities, assets and operations. They then consider the building's current network architecture and cybersecurity risks, rules and regulations, to show how a secure system would look. This knowledge is distilled into a roadmap that identifies the steps needed to move from the current state to a connected building that operates in a safe and secure fashion. However, making that shift a reality requires the right organisation to be put in place, including allocating clear responsibilities and ownership for cybersecurity, which are still lacking in many real estate companies.

For example, the complex security ecosystem of a smart building involves many parties: the asset owner, the integrator of the technology, the building operator and the technology manufacturers. Devices must be manufactured, specified and procured to suitable security standards (including passwords and encrypted communication), configured by the integrator to work to the same standards across all devices and systems, and operated under policies and procedures that preserve security through updates and maintenance. All parties must therefore work together in a co-ordinated way to ensure that the building is truly secure.

Without a strategic approach, cybersecurity can become a fire-fighting exercise, reacting to each new threat with a different tool, which can lead to overspending. The threat landscape of today might be different in ten years, or three months, or two hours, so security activities – such as intelligence-gathering, due diligence and penetration testing – must be an ongoing responsibility. By establishing pre-emptive awareness and adaptation as routine processes, a well-designed security organisation will take cyber-obstacles in its stride.



Regulation, collaboration, opportunity

Furthermore, besides the need for building effective security, companies now face the challenge of demonstrating compliance. For example, the EU's Network & Information Security (NIS2) initiative aims to achieve a consistent level of cybersecurity in critical sectors across all member states, while the Cyber Resilience Act (CRA) will establish security standards for digital devices. However, just as with sustainability regulations, the right strategic perspective can turn a compliance obligation into a business opportunity, to develop effective and resilient building management systems.

Another parallel between cybersecurity and sustainability is their greater focus on collaboration, using openness and transparency to promote sector-wide best practice. Although concealing any cyber vulnerabilities or attacks might appear to protect market confidence, the most effective responses to cyber-attacks have in fact involved making them public, and sharing the key learnings more widely.

Smart buildings are the future of real estate but, for them to deliver their commercial and sustainability benefits, they must also be built on a solid foundation of robust cybersecurity.

Authors

Jeroen Slobbe
Senior Manager
jslobbe@deloitte.nl
Deloitte The Netherlands

Katinka Kruseman Aretz
Manager
kkrusemanaretz@deloitte.nl
Deloitte The Netherlands

Taede Rakhorst
Partner
NL Emerging Tech lead
trakhorst@deloitte.nl
Deloitte The Netherlands

Designed by CoRe Creative Services. RITM1598755