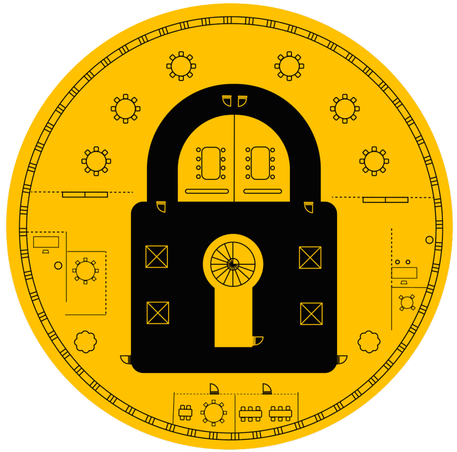
Deloitte.



Cyber risk in the building lifecycle: Smarter buildings will know more about us

With modern buildings depending more and more on technology and becoming more and more interconnected, numerous questions are arising about their resistance to cyber risks. To optimize management and increase cost-efficiency while ensuring access to adaptable and comfortable living and working space, buildings are collecting and processing information not just about the structure itself, but about us – including such technical and private data as names, IDs, photos, and videos. Protecting this data – from generation to storage to disposal – must be a critical part of the new, smarter building management systems. To do this, real estate companies, third-party suppliers, and IT companies must embed *secure by design* and *privacy by design* rules into their building development lifecycle.

Written by:
Marcin Ludwiszewski (PL)

Threat landscape

In their strategic planning, real estate companies need to understand their business risk profile and threat landscape. Smart buildings and building management interfaces may be exposed on the Internet, attracting not only the attention of the occasional hackers who may only "check" if systems are vulnerable (not necessarily knowing if they cause any disruption) but also of financially motivated criminal groups that act to extort money. They could simply change the way the building operates, making it unavailable to tenants, visitors, or third parties, or even affect health and safety. Including a threat intelligence and risk analysis in strategic planning will be fundamental for real estate companies in recognizing such threats and in responding to them through the development and adaptation of their security perimeters.

Cloud security

Traditional on-premise systems like CRM, ERP, sales, finance, budgeting, or reporting are all being transitioned to cloud, which can improve long-term forecasting and planning processes. But while the cloud offers numerous advantages—such as centralized management, scalability, reliable data storage, and enhanced automatic processing—the transition can pose cyber risks. A cloud security analysis should be part of the cloud transition strategy, and a security risk analysis should be performed in case of any major changes in the business or in the supporting technology.

Interconnectivity

New buildings may incorporate standard protocols that will facilitate data exchange with other smart buildings, smart city ecosystems, third parties, suppliers, or even tenants, extending the potential attack surface. This clearly raises questions about how this information is protected in transit, how the connected systems or interfaces are protected, or even whether the connected suppliers increase the risk profile. Tenants and suppliers alike will need to adhere to specific security requirements to be connected so that real estate companies are capable of managing their risks throughout the contract lifecycle. What is more, real estate companies will need to develop mature capabilities and cooperate with third parties and tenants not only to prevent but also to detect and respond to cyberattacks.

Cyber resilience

Buildings will know not only what we do but how and when we do it. We will be recognized by the building every time we appear in the office (facial biometric recognition for commercial and office space is now a fact). The question is, what happens if a visitor is not recognized by the building? Would anyone be able to control the way the building reacts to specific people? How can tenants be sure the building is resilient to cyberattacks?

To respond to these real concerns real estate companies will have to adopt security practices that until now have mainly only been followed by the financial industry and other risk-sensitive sectors. Activities such as red teaming or cyberattack simulations can help real estate companies verify whether they are resistant to cyberattacks and whether their personnel is alert to such threats, properly trained, and capable of responding effectively.