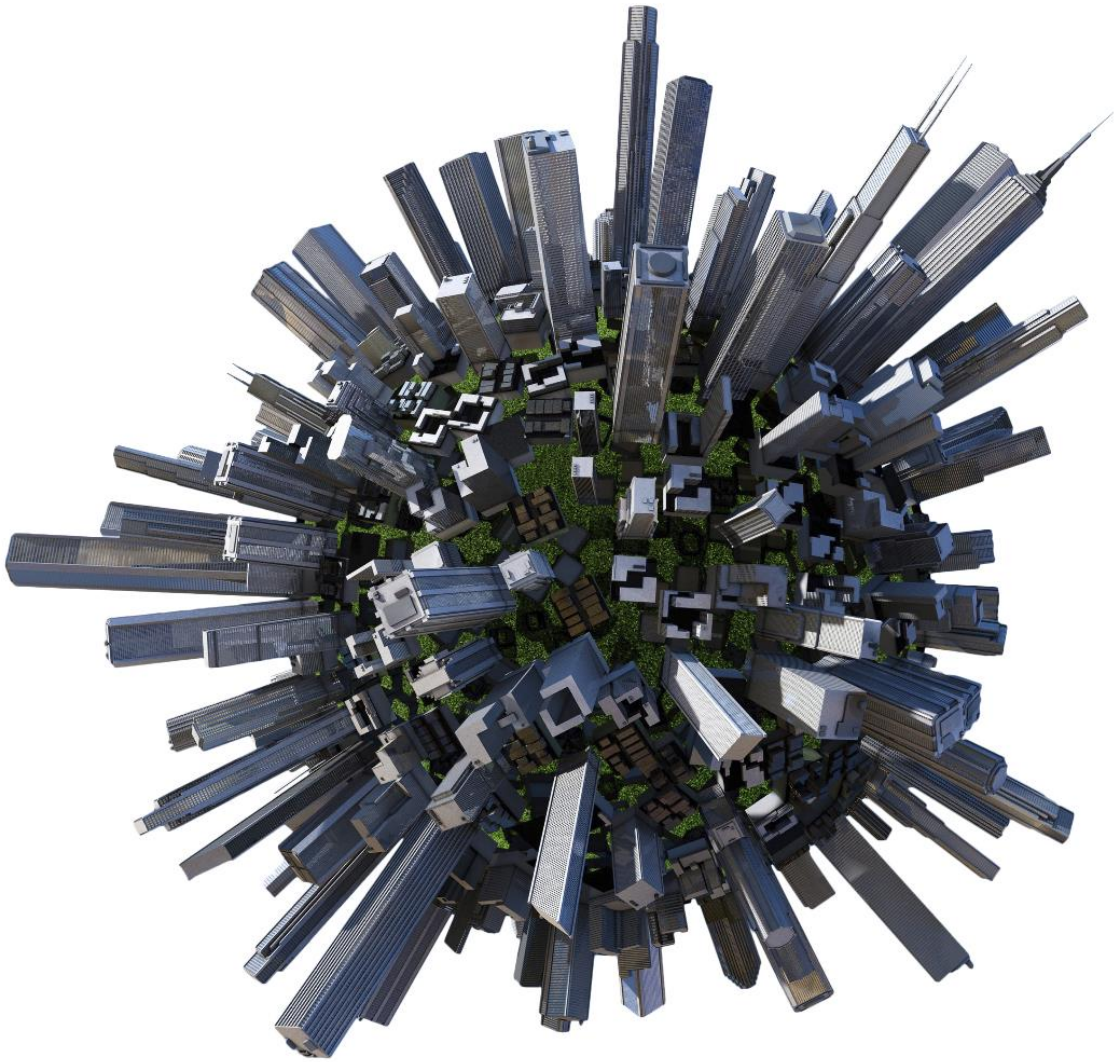
Deloitte.



Real estate predictions 2017

What changes lie ahead?

Cyber Risk

Cyber Risk

Rising cyber risk in real estate through the rise of smart buildings

Technology-driven innovation is the order of the day, and through this firms of all types seek to create competitive differentiation. We expect a rise in smart buildings, driven by new technology, sensors, the Internet of Things and by new workplace strategies of firms. Smart buildings are becoming critical to competitive advantage and can also open new revenue streams, energy efficiency and sustainability. However, with the rise of smart buildings new risks emerge as well. One of the most important to consider is cyber risk.

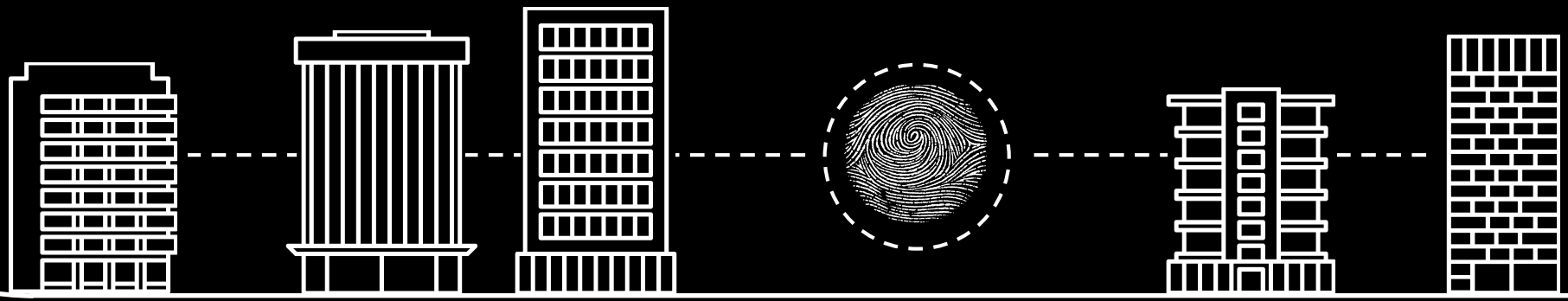
January 19, 2017

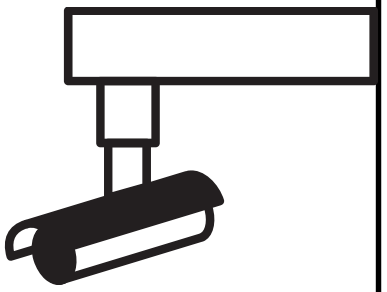
Industries like retail, travel and hospitality, and the financial services industries have long been dealing with cyberattacks, and have not only matured their response capability but also positioned cybersecurity as a core element of their businesses. In contrast, the commercial real estate (CRE) sector considers itself to be relatively less at risk from a potential cyberattack. This is because CRE firms typically maintain relatively less consumer personally identifiable information (PII) and valuable intellectual property (IP) directly on their own technology systems. However, due to the rise of smart buildings where tenants have building management systems on their smart phones, new opportunities for cyberattacks will emerge within the sector. The interconnectedness of real estate owners' systems and tenant IT systems form a potential cyber risk for both parties. As a consequence to this heightened risk we predict IT and CRE will become more intertwined during the coming year to face these new cyber threats.

The rise of smart buildings

CRE firms must advance their use of new technologies such as cloud, mobile and social media to drive tenant engagement and operational efficiency. In addition, they must implement increasingly sophisticated technological solutions for building management systems (BMS). Some commonly used solutions of this type include systems to automatically control heating, ventilation, air conditioning, lighting and safety systems. The increased use of digital technologies also exposes information and data through multiple channels. At a corporate level, web-based transactions with tenants and vendors, use of cloud services, the growing use of smartphones and tablets under bring your own device (BYOD) policy, and social media presence create multiple access points for the PII data stored by CRE companies.

At an asset level, the interconnectedness through internet-based networks, industrial control systems HVAC and open Wi-Fi networks increase data vulnerability. These asset-level cybersecurity risks do not only apply to CRE owners. Smart buildings tend to be interlinked with tenant systems, creating exposures to tenants whereby their systems and data can be accessed through the CRE owners' IT systems. Therefore, cybersecurity is a key consideration for modern day buildings.





Smart buildings need more protection

The data that is generated by a smart building can be considered as an asset and will lead to new business models and revenue streams. However smart buildings also need more protection than the traditional security systems of a building. The cost of multiple million Euros on average per company.

According to analysis by the Deloitte Center for Financial Services, the most visible objective for cyberattacks on CRE companies has been the theft of PII and other sensitive information, as well as IP, such as strategic plans, engineering drawings, and tenant information. Furthermore, CRE companies may be uniquely vulnerable to treasury management cyber risk, given the significant amounts of cash maintained on the balance sheet as well as large Euro transactions related to acquisitions, dispositions, and financing of real estate properties. Many CRE companies have expressed concern about potential cyber vulnerabilities in wire transfer processes associated with these large Euro transactions. Here, we believe that organized criminals and/or insiders could be the most significant potential threat actors.

When it comes to tenants, the interconnectedness of their IT systems with CRE owners' systems as described above, creates several vulnerabilities for them as well. Perpetrators can use the IT systems of the physical asset as an attack surface to cause physical destruction, reputational damage, financial, and/or productivity loss to the tenant. Organized criminals, nation states, hacktivists, or terrorists can destroy critical infrastructure by compromising BMS that can impact both safety of the environment and human life.

Top three risks

In summary, the analysis suggests that the top three risks that the CRE sector should be aware of and prepare for are:

1. Theft of PII data

2. An attack on tenants through building systems

3. Destruction of physical infrastructure

In 2017 the focus will be on properly addressing the associated cyber risks which allows CRE firms to keep innovating at a rapid pace, recognising that not just their own office infrastructure but even the buildings they develop are effectively now IT assets instead of only brick and mortar.

For more details we refer to the report: 'Evolving cyber risk in commercial real estate'.

Cyber Risk Quantification

Deloitte analyzed and quantified cyber risk and the associated value loss for all major Dutch sectors. Get more insight on the drivers behind these cyber risks to better understand how cyber risk may emerge in Real Estate and download our reports on the risk drivers Beneath the Surface of a Cyberattack as well as overview across Dutch sectors on the Cyber Value at Risk in The Netherlands.

Deloitte.