Smart buildings, smart cybersecurity solutions

Inhoud

Inleiding

Smart buildings contain more and more interconnected installations and systems. While these innovations improve efficiency and sustainability, they introduce significant cybersecurity risks that require attention and precautions. New regulations in the field of Environment, Social and Governance (ESG) are also forcing organisations to be more efficient with risk and compliance management.

At the same time, the needs of society and the client are changing. Sustainability ambitions and technological innovations require the integration of new technology in buildings. The new generation in the labour market and digitisation are changing the relationship between building and user. The solution is often sought in further digitisation with the aim of a smart integrated building.

A survey of CFOs of real estate organisations found that 97% of organisations are actively interested in applying AI within their building and 72% are actively engaged in it to a greater or lesser extent[1]. Investment bank JP Morgan expects the global smart building market to grow by 10% annually in the coming years to reach a total revenue of USD 205.3 billion by 2031[2]. An underexposed topic is what these great innovations mean for the cybersecurity of smart buildings. In this article, we explore which innovations are being implemented in concrete terms and what you need to think about when it comes to cyber risk management. Finally, we conclude with recommendations for daily practice.

[1] *AI in Real Estate, Brent Horak, Kristi Gibson and Kirstie Tiernan, BDO USA,* *https://www.bdo.com/insights/industries/real-estate-construction/ai-in-real-estate*

[2] *Outlook 2025 - wealthmanagement, JP Morgan, https://www.jpmorgan.com/content/dam/jpmorgan/documents/wealth-management/outlook-2025-building-on-strength.pdf*

Smart buildings

How do the above developments translate into a smart building? If we zoom in on the sustainability issue in buildings, we see the following network-connected components, among others:

- solar panels for generating electricity
- batteries for storing electricity
- charging stations for dispensing electricity
- smart meters for minimising the cost of electricity
- smart lighting/HVAC systems to reduce the consumption of electricity within a building
- security cameras
- access control systems.

In addition, the use of a digital twin can be used for advanced data analyses, so that leaks or draughty spaces can be discovered earlier. This can contribute to combating (energy) waste.

For the more efficient design of the building, we see that sensor technology can measure wear and conditions, and this data can then be used to optimise maintenance[3]. The cleaning robot and in some cases a security robot have also made their appearance. Remotely reading and operating measurement and control systems (e.g. of the elevator, escalator, or HVAC systems) reduces the trips that a technician must make to a building. As a result, fewer people can keep an eye on more buildings, which is not an unnecessary luxury in these times of a tight labour market.

For the user, we see that the same sensor technology can be used to identify available workplaces, parking spaces or meeting rooms in the building. This data can also be used by the landlord to make a better estimate of the space required. After all, fewer square meters mean a lower bill. And a better occupancy rate means more revenue at the same cost. In addition, infotainment systems are introduced, which, for example, display the latest news from the organisation or show when the train/bus is leaving, so that employees can adjust their travel schedule accordingly.

Finally, smart buildings offer additional opportunities for the (physical) security of the building. Smart cameras, fire detectors, security robots, doors, and motion sensors introduce the possibility for a next-generation security system.

[3] *Future-proofing infrastructure: leveraging AI and analytics for a competitive advantage, Chetan Sehgal, Roshan David, Bill Syrros, BDO Canada,* *https://www.bdo.ca/insights/future-proofing-infrastructure-leveraging-ai-and-analytics-for-a-competitive-advantage*

Cyber risks

A good question to ask is: what is the core functionality of the building and what impact does the building have on the end user's operation? A prison simply has a completely different risk profile than a factory, safe, primary school, or hotel chain. For example, the solution to a ransomware attack on an office building[4] may be to allow staff to work from home for a while, but in a similar attack on the HVAC systems in a hospital building[5], a very cold or very hot room may be problematic for the patient.

Last year, a hotel chain was hit by ransomware[6]. Because the digital pass system was also affected, there was a direct impact on the hotel's operations, because of which the revenue-generating activity (renting out rooms) had to be stopped. A similar pass system turned out to be vulnerable to an attack[7], which meant that the safety of the visitors' belongings could not be guaranteed. This can have an impact on a hotel's reputation but can also lead to claims if this system is abused.

Last year, prisons were also on the radar. Whereas in 2011 vulnerabilities in doors were already reported[8], this year it was hit with tracking devices that were used to improve the safety of security personnel during their work [9]. In addition, the layout of a prison leaked[10], which may pose a risk to the primary function of the building. Various energy systems were also in the spotlight this year.

[4] Case: One wrong click can create a 92-day Recovery, IFMA, https://ifma.foleon.com/white-paper/cybersecurity/case-one-wrong-click

[5] Alleged HVAC Hack Shines Spotlight on OT Risks to Healthcare, Marianne Kolbasuk McGee, Healthcare information security, https://www.healthcareinfosecurity.com/alleged-hvac-hack-shines-spotlight-on-ot-risks-to-healthcare-a-17320

[6] Omni Hotels experiencing nationwide IT outage since Friday, bleepingcomputer, https://www.bleepingcomputer.com/news/security/omni-hotels-experiencing-nationwide-it-outage-since-friday/

[7] Hackers Found a Way to Open Any of 3 Million Hotel Keycard Locks in Seconds, Wired, https://www.wired.com/story/saflok-hotel-lock-unsaflok-hack-technique/

[8] Vulnerability allows hackers to open prison doors, hiding activity from central command, venturebeat, https://venturebeat.com/business/prison-door-hack/

[9] Jailbreak fears as prison maps are leaked on the dark web, The Times, https://www.thetimes.com/uk/crime/article/leak-of-prison-layout-plans-lead-to-drugs-and-escape-fears-ddg6d9lz6

[10] tracking devices on prison vans disabled after cyber-attack, Financial Times, https://www.ft.com/content/84753e89-b769-42fb-ac85-a76b91c3fe1f

For example, the NOS reported that solar panels contain a large number of vulnerabilities[11] and that there are concerns about future attacks on batteries[12]. In addition, there is the standard concern that energy will be stolen[13], a scenario that could also be achieved via cyber[14]. The question here is what the impact is for the owner of the building. If the building is also connected to the regular grid, this will have an impact on the finances and sustainability reporting.

A completely different risk for a smart building is the risk of violating laws and regulations. There are a number of laws that may affect the cybersecurity aspects of a smart building: the General Data Protection Act (GDPR), the Network and Information Security Directive (NIS2) and the Cyber Resilience Act (CRA). The GDPR[15] sets requirements for the collection and processing of personal data. For example, the use of camera images for purposes for which there is no approval, or not having carried out a Data Privacy Impact Assessment, can result in a violation. The new NIS2 [16] may also apply, for example in the case where the building supports (primary) functions for public and private entities that provide essential services or carry out activities that are crucial for the continuity of these services (e.g. a prison, hospital building or safe). Finally, it is recommended to look at the Cyber Resilience Act (CRA)[17]. This sets requirements for placing products with a digital element on the European market. How will parties that import components for smart buildings (elevators, solar panels, CCTV cameras, screens, HVAC systems, batteries, smart locks, infotainment systems, etc.) ensure that there are enough suppliers to supply these products compliantly?

In summary, we can distinguish a number of main risks. A cyber incident within a smart building can result in the main functionality of the building not being available. Depending on the function of the building, this can be very serious or especially annoying. From a commercial point of view, the result may be that fines for downtime have to be paid or that less invoicing can be done because fewer m^2 are available. Another important risk is non-compliance. Depending on which law is violated (GDPR, NIS2), fines can be imposed and there may even be administrative liability. In addition, there is a risk of liability if a cyber-attack affects the end customer via the smart infrastructure of the owner of the building[18]. A cyber-attack can have an unimaginable impact. The operational processes can come to a standstill for days, mean direct financial damage, emotional impact on those directly involved, impact on other stakeholders of the organisation.

[11] Solar panels susceptible to hacks and failures: 'Hack power grid is realistic', NOS, https://nos.nl/artikel/2477039-zonnepanelen-gevoelig-voor-hacks-en-storingen-hack-stroomnet-is-realistisch

[12] Increase in battery use increases risk of cyber attack, NOS, https://nos.nl/nieuwsuur/video/2550410-toename-gebruik-batterijen-vergroten-risico-op-cyberaanval

[13] Systematic review of energy theft practices and autonomous detection through artificial intelligence methods, E. Stracqualursi et. al, Sciencedirect, https://www.sciencedirect.com/science/article/pii/S136403212300401X

[14] Smart meters can be hacked to cut power bills, BBC, https://www.bbc.com/news/technology-29643276

[15] User Privacy Concerns and Preferences in Smart Buildings, Harper et al, Socio-Technical Aspects in Security and Trust, https://www.researchgate.net/publication/352566018_User_Privacy_Concerns_and_Preferences_in_Smart_Buildings

[16] Cyberbeveiligingswet (NIS2-richtlijn), NCSC.nl, https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

[17] De Cyber Resilience Act: Hardware hacking and product security, Jeroen Slobbe, NOREA, https://www.norea.nl/magazine/de-cyber-resilience-act-hardware-hacking-en-product-security

[18] Target Hackers broke in via HVAC Company, Krebs-on-Security, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Smart solutions

To ensure that the great innovations go hand in hand with practical cybersecurity solutions, we recommend that organisations invest in the following activities and organisational structures:

Governance: with different actors in the field, it is important to clarify who is responsible for what and what exactly this entails. The Singapore standards division[19] is in the process of developing a specific standard for smart buildings (TR 111:2023). This standard is based on well-known engineering security standards (IEC 62443-3-3, 4-1 and 4-2) and thus helps to work out the technical requirements for systems, components, and the development cycle. A European variant would be useful. Organisations can also (depending on their role in the ecosystem) embrace and implement these standards. It is also important to clarify roles and responsibilities within the organisation. Who takes care of the procurement of safe and CRA-compliant components? Who keeps an overview of the assets in the portfolio and reports on risks in (large) projects?

Security Architecture of Operational Technology (OT): a good OT security architecture can help to properly align different interests. It provides insight into which system should communicate with which system, what the risks are, but also which capabilities have been implemented to mitigate risks. A good building management system (BMS) security architecture can also be a means of communication towards leadership to communicate risks, justify the licensing costs of solutions (such as antivirus solutions, patch management, vulnerability management, security monitoring, End-point-Detection and Response (EDR), Backups, Multi-factor authentication (MFA), etc.) and provide an overview of how the security vision and smart building vision will come together in the coming years.

Monitoring: an important pillar within cybersecurity is monitoring systems. There are already many standard products for this for the IT infrastructure, but for specific building management systems this is still in its infancy. It is important to test solutions through pilots and future-proof systems so that incidents can be discovered. Which building-specific detection cases can already be written based on the available information? Can we make this information available in a smart and secure way? If so, the first steps can already be taken.

Awareness: in addition to the usual information security awareness sessions, it is important to draw specific attention to the cybersecurity of OT components. This can be done by means of an extra module in the standard e-learning for maintenance employees, for example, but the great thing about OT systems is that it can easily be made very tangible. Building a specific demo and showing the impact of a hack and what a security check does makes it tangible for employees who work with the systems. It also helps in building the bridge from IT (security) professionals to the construction engineers and maintenance engineers. By connecting both worlds better, mutual understanding is created, which results in better solutions in the field.

Penetration testing: finally, we recommend that organisations periodically test the systems. This can be done by carrying out a pen test just before the delivery of the building, in consultation with the owner of the building when it is in use, or even at component level even before it is realised in the smart building concept. During a penetration test, the technical reality, and the strategic and policy world meet. A good test provides insight into the resilience of the building network and various components and also provides important insights into how the technical implementation can be refined.

[19] *TR 111:2023 securing cyber-physical systems for buildings, Singapore Standards, https://www.singaporestandardseshop.sg/Product/SSPdtDetail/98cf35ec-5e5b-4850-a0f5-04fa148aac29*

Conclusion

The rise of smart buildings brings numerous benefits, including improved sustainability, efficiency, and safety. However, these technological advances also come with new cybersecurity risks that should not be overlooked. By investing in cybersecurity, organisations can live up to society's trust in these solutions. Nowadays, the safety of a building goes beyond good hinges and locks, locking windows and doors when the last user leaves a building on a working day and having technical and safety systems in order. The IT environment of a building must also be conclusive! Every improvement starts with gaining insight. Insight into the current situation and the goal, in other words: the desired situation. Insight is the beginning of targeted improvements. Identifying bottlenecks, vulnerabilities and especially unaddressed risks are the starting point for the improvements on the way to a deliberately chosen higher level of cybersecurity within your organisation. It is also important who bears what responsibilities and liabilities.

More information

If you want to know more about how you can efficiently reduce cyber security risks of smart buildings, please contact our professionals!

JEROEN SLOBBE
Director BDO Digital – Cybersecurity Advisory
jeroen.slobbe@bdo.nl
+31 6 - 82 01 92 40

ARJAN ENDHOVEN
Partner BDO Tax & Legal – Chairman of the Real Estate & Construction Industry Group
arjan.endhoven@bdo.nl
+31 20 - 543 21 00

www.bdo.nl

02/2025 – BM2514

A different view on value