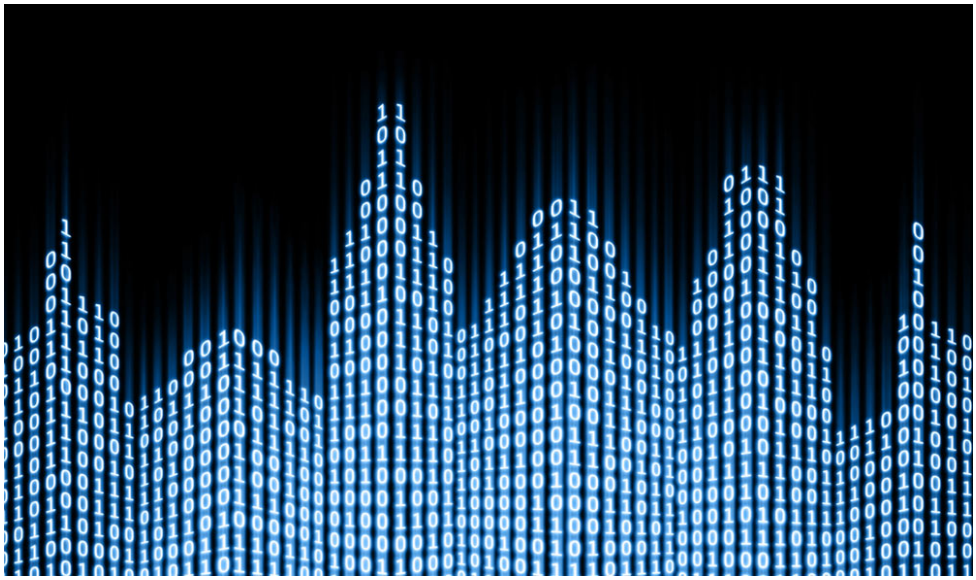
THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES



RISK & INNOVATION

Smart Building Technologies: Balancing Value And Risk

OVERVIEW

You arrive at the office, tap your ID card to call an elevator, go directly to your floor, and then settle into your climate-controlled office. Nothing about that seems particularly remarkable.

But in just that short period of time — from entering the building to sitting at your desk — you've walked through multiple hidden layers of sophisticated technology. The elevator didn't stop at unauthorized floors. The heating, ventilation, and air conditioning (HVAC) system switched over from its overnight energy-saving mode to the comfortable settings you enjoy during the day. Meanwhile, tens of thousands of sensors monitored your building's mechanical systems, calling in a repair engineer to carry out preventative maintenance. Automated security systems reduced the building's vulnerability through constant monitoring.

For building owners, technology's appeal is obvious: IBM notes that operations take up 71 percent of a building's total cost over its lifespan. Data automatically informs building operations, enabling cost savings while providing more amenities, increased safety, and greater comfort for occupants. And since smart buildings are more profitable, these technologies also increase the value of real estate.

However, this convergence of the physical and digital worlds calls for a different approach to risk—one that breaks down organizational silos.

"Organizations that are ahead of the curve are already treating these systems as critical IT infrastructure," said Stefan Toi, Senior Broker at Aon. "This means they reap all the benefits that come with this, including access to experienced IT teams that will work to remove the weak links in the infrastructure."

And weak links could prove costly. The tech that brings great benefits to building owners and occupants also provides points of entry to hackers.

The challenge for building owners is: How can they capitalize on the opportunities of smart technologies while addressing the increasing number of risks?

IN DEPTH

Technology is transforming modern buildings from inanimate bricks into self-contained ecosystems. Smart buildings can control every aspect of their operations: Blinds automatically lower for the sun; sensors track foot traffic; motion sensors and cameras replace security guards. New applications transform the management and efficiency of the HVAC system, elevators and escalators, security and safety, water use, and building access.

And the benefits aren't without risk. Earlier this year, the Austrian hotel Romantik Seehotel Jaegerwirt was hit by a ransomware attack, with hackers disabling the hotel's keyless entry system and locking guests out of their rooms. The results were simply an inconvenience, a relatively benign outcome given the possibilities. But the next time, hackers could use such vulnerabilities to damage property — such as shutting down elevators or endangering occupants by remote-locking rooms.

What this incident demonstrates is that a building's increasing reliance on technology presents significant risks to critical systems.

The Rise of Convergence

Thanks to smart technology, physical risks are converging with cyber exposures. "Traditionally, physical and cyber security have operated as two very distinct functions," said James Morris, Regional Security Manager, EMEA, at Aon. "Physical has focused on keeping people and property safe, typically reporting through an operations, administration or legal-type function. Meanwhile, cyber focuses on the information asset side, through the overall technology leadership."

That sort of approach made sense in the past, Morris said, but it needs to change in the era of smart buildings and the Internet of Things (IoT). "There's a growing need to consider the two functions together. The risks that modern businesses face no longer occur in isolation so they cannot be treated in isolation."

The risk of cyber attacks, and the cost of defending the building against them must be factored into any analysis of smart technologies. Only then can property owners accurately gauge the return on their investment. In the same way that security breaches of customer information in banking or retail can affect sales and profits, cyber attacks on vulnerable buildings could (in theory) reduce property values.

A Smart Path Forward

Now that the benefits of smart buildings are evident, there's no way to put the genie back in the bottle. The real estate industry's use of smart technologies, sensors, and IoT will only increase in the years ahead. A recent Deloitte Center for Financial Services study examining connectivity in commercial real estate found that sensor deployment in the sector is likely to grow at a compound annual growth rate of 78.8 percent from 2015 to 2020, reaching nearly 1.3 billion sensors.

"As buildings become ever more interconnected, the number of entry points for would-be hackers is only set to increase," said Toi. Too often, though, smart building systems aren't subject to the same security governance as traditional IT systems, Toi explained.

Now that physical and cyber risks have become intertwined, building owners should take a comprehensive view of security risks across an enterprise's interdependent business functions, Morris said, along with the development and integration of appropriate risk solutions and mitigations.

Smart buildings are just one component of the interconnected world of smart cities, so the concept of convergence is instrumental in managing the risks as the built environment becomes more tech-infused.

Keeping Pace With Technology

"The rapid development of smart building technology coupled with the ever-evolving nature of cyber threats makes it difficult to maintain a responsive and relevant risk management framework," said Andrew Mahony, Regional Director, Financial Services and Professional Group, Asia, at Aon.

Mahony, along with Australia-based Troy Bates, a Client Manager focusing on the real estate industry, recommend that state building owners and risk managers should explore:

- Changes to digital access points and authentication hot spots, particularly for vendors and tenants
- How the introduction of new technology into the smart building increases exposures
- Data sharing or digital platforms between tenants and the smart building
- The extent to which building control systems are connected to communications systems
- The contractual risk management framework, including any provisions that call for building management to assume liability for data or system performance or for transferring liabilities.

"Armed with that information, smart building managers can develop dynamic incident response and business continuity plans," Mahony said. In addition, as reliance on automation and connectivity grows, building owners and managers should consider more frequent cyber risk reviews, along with crisis simulation exercises involving internal stakeholders and external vendors. An example would be a network disruption in which a smart building's systems are compromised, affecting building functions and preventing tenants from conducting business.

Smart building owners can also learn from the experiences of other sectors. In the power and manufacturing industries, for example, companies "airgap" — or quarantine — control systems and communications systems. Such airgapping is an attempt to limit malicious access to systems in which physical risk converges with cyber exposure. But no approach is foolproof. Airgapped systems can be compromised by advanced threats, rogue insiders, and even the inadvertent actions of well-meaning employees.

Ultimately, the best line of defense for a smart building is a well-informed, dynamic, and comprehensive risk management framework.

Smarter Buildings Calls For Smarter Building Management

Smart building technologies are on the verge of mass adoption. A recent report predicted the global market for smart buildings will grow from $5.73 billion in 2016 to $24.73 billion by 2021. The technologies are becoming more impressive by the day. Buildings now include features from thermal systems that passively distribute heat over the course of a day, to smart LED panels that monitor and report detailed humidity and temperature readings. Whether a retrofitted historic building or gleaming new structure with state-of-the-art systems, the more smart buildings rely on new technologies, the greater the associated risks.

Building owners who focus solely on the cost savings and convenience of smart building technologies might be leaving themselves exposed. An effective risk management strategy that accounts for the convergence of physical and cyber exposures is the best way to reap the full benefit of these technologies.

TALKING POINTS

"Changing mindsets, policies, and technologies to create secure connected buildings will take time, effort, and investment. In the meantime, companies must start paying attention to the potential cybersecurity risks within their physical spaces in order to protect their building, employees, and data." – Paul Ionescu, ethical hacker

"Any security breach in the Internet of Things cannot only severely affect the digital world, but more importantly might lead to grave safety issues in the physical world. Security and safety are tightly integrated, exacerbating relevant threats and risks." – Udo Helmbrecht, Executive Director, European Union Agency for Network and Information Security

"No amount of regulation can force companies to maintain old products, and it certainly can't prevent companies from going out of business. The future will contain billions of orphaned devices connected to the web that simply have no engineers able to patch them." – Bruce Schneier, Chief Technology Officer, IBM Resilient; Fellow at Harvard University's Berkman Klein Center for Internet & Society

FURTHER READING

- “Smart” Cities And Buildings: The Emergence Of The Cyber Safe Building — The Urban Developer, July 18, 2017
- 5 Technologies That Are Making Smart Buildings Smarter — Construction Dive, November 2, 2016
- Top 8 Smart Buildings From Around The World — Comfy Blog, February 21, 2017
- How To Avoid A Cyberattack: Real Estate Checklist — Commercial Property Executive, August 8, 2017
- 10 Companies Moving Up In Smart Buildings — GreenBiz, December 19, 2016