

Picture credit: Adobestock

DESIGN FOR LIFE

Richard Hilson reveals why *every smart building needs a security-first design strategy*

One of the biggest challenges for architects and developers right now as they continue to embrace smart building technology, is that every connected system is also opening potential vulnerabilities. How to stay connected, and resilient. Drawing on insights from the SIA's 2026 Megatrends Report, this feature explores how architects and specifiers are successfully implementing security into design – rather than as a late-stage technical addition.

From IoT-enabled access control and touchless entry systems to integrated building management platforms, modern buildings are fast-becoming interconnected ecosystems as we seek improved efficiency, sustainability and user experience. But, while we start to realise the efficiencies we crave, we need to stay ahead of the curve, and the criminal, from a design perspective.

The SIA report offers a great helicopter view of where the built environment is heading. No longer conceptual or the vision of 'tomorrow's world', AI-driven automation, connected infrastructure, cloud-managed systems and unified security platforms are rapidly transforming how buildings are designed, accessed and operated.

A consideration for architects and specifiers however, which the report raises, is around whether buildings are becoming smart faster than they are becoming secure? Across commercial developments, public buildings and critical infrastructure, connected technology is now deeply embedded into everyday operations. Access control systems are managed via smartphones and mobile credentials, while sensors monitor occupancy, energy usage and environmental performance in real time. Likewise, building management systems increasingly control lighting, HVAC, lifts and surveillance. All this is delivering enormous operational benefits, but it is also reshaping risk and introducing vulnerabilities.

A significant trend is the adoption of AI-driven automation across security and operations, which is moving at a heady pace as smart buildings become autonomous. Systems can now automatically adjust environmental controls based on occupancy, identify unusual access patterns, optimise energy usage and trigger alerts without human intervention. But this also creates dependency, which us mere humans take for granted. Disruption to one platform can quickly affect wider operations and, if an automated building management system is compromised, manipulated or taken offline, the consequences can extend far and wide.

The National Cyber Security Centre (NCSC) and The Cybersecurity and Infrastructure Security Agency (CISA) in the USA have been quite vocal on the risks to smart infrastructure, highlighting how poorly secured operational technology environments are becoming attractive targets for cybercriminals. But it's one thing to understand operational vulnerability, yet another to design an intelligent, or smart, environment with processes in place to combat it.

Another major trend is the growth of unified platforms, where multiple building functions are integrated into single operational ecosystems. Access management, surveillance, visitor systems, HVAC controls and occupancy management can now operate through interconnected platforms designed to streamline operations and improve visibility. All of which are transforming the user experience, and ultimately improving public safety.

But we must be wary that the removal of silos, including those which saw physical and cyber security operating independently, can also create concentration of risk. Especially now we see hybrid threats across physical, cyber and aerial domains. For instance, a compromised access management platform could potentially affect physical entry points across an entire building. A vulnerable building management system may provide pathways into wider corporate networks. And increasingly, cyberattacks are targeting operations, not just data.

There have been well-documented cases of breaches through smart technology, too. Albeit around seven years ago, one infamous incident involved cybercriminals gaining access to a North American casino network through a smart fish tank thermometer, ultimately allowing them to extract sensitive data from the organisation's systems.

In addition, the UK's National Protective Security Authority (NPSA) has highlighted how HVAC systems and building automation controls can create potential vulnerabilities within modern buildings if security is not properly considered. It warns that building automation and control systems should be carefully secured, with organisations needing clear oversight of who can access and control systems remotely.

As smart infrastructure becomes more deeply embedded within commercial developments, building resilience is increasingly dependent on securing both physical and digital environments together. And the risk escalates, with (massive) IoT, which is designed to extract data from multiple, potentially hundreds of thousands of smart technology points, in commercial and domestic settings across the globe.

Smart technology is becoming a standard expectation within many commercial and public sector environments now, especially as we strive for a 'frictionless' user experience, and convenience. This is changing how buildings are being specified and at the same time, ESG priorities are driving the use of smart sensors and automated energy management systems designed to optimise performance and sustainability.

However, the IBM X-Force Threat Intelligence Index highlights how operational technology and connected infrastructure environments are becoming increasingly attractive targets because of the disruption attackers can cause through them. Likewise, many smart buildings still rely on legacy operational technology and outdated software environments, creating additional vulnerabilities when integrated with newer connected platforms.

CONNECTED TECHNOLOGY IS NOW VERY DEEPLY EMBEDDED INTO MANY EVERYDAY OPERATIONS

The challenge here for architects and developers is one of convenience and connectivity over resilience. Namely, are buildings being designed around operational efficiency without sufficient consideration of recovery, fallback and system segregation? Personally, I think we've moved way past this and have much greater focus upon the holistic approach, which incorporates operations and security across all layers.

Today, architects and specifiers are playing a much more influential role in shaping how resilient buildings become. Decisions around integration platforms, infrastructure pathways, connectivity, access flows and operational technology now directly influence long-term security. This is particularly relevant in commercial real estate, healthcare, transport, energy, data centres and critical infrastructure environments where continuity is absolutely vital and has become just as important as physical protection.

The goal is to create buildings that are both intelligent and resilient – environments where security is embedded into design from the outset, rather than retrofitted later in response to emerging threats. From what I hear in my everyday conversations with prospects and suppliers, that is very much the case. We are ahead of the curve and we need to be, because the curve will always be where the threat, the criminal mind, is.

The future of smart buildings will not be defined solely by how connected they become, how easy it is for people to move around or how technology has forged forwards like a reconnaissance mission ensuring everything is ready when a visitor or member of staff arrives. I believe they will be defined by how resilient they are designed to be and as buildings continue to evolve into interconnected digital ecosystems, physical and cyber security will become increasingly intertwined.

This also means resilience, access governance and security need to be considered alongside sustainability, efficiency and user experience from the earliest stages of design. Because the smart buildings of the future, those that haven't even entered the mind let alone the drawing board, will undoubtedly be more intelligent, more automated and more connected than ever before ●

The IBM X-Force Threat Intelligence Index highlights how operational technology and connected infrastructure environments are becoming increasingly attractive targets

Richard Hilson is Business Development Manager at PFL – Access Management.