Creating Resilience

Protecting the Portfolio: Strengthening Building Resilience Against Next-Gen Cyber Threats

VIEWPOINT

CBRE RESEARCH
JULY 2026

Introduction: A New ESG Imperative

Recent years have seen cybersecurity emerge as a fundamental component of comprehensive sustainability and Environmental, Social, and Governance (ESG) risk and impact analysis as the severity of digital threats escalates beyond merely being an IT issue to become a significant corporate oversight failure.

Corrado Forcellati
Senior Director
ESG Consulting & Sustainability Services
Head of Paia FROM CBRE
Asia Pacific

Despite growing awareness, most commercial real estate landlords in Asia Pacific are not prioritising cybersecurity in their portfolios. This is despite the deployment of Internet of Things (IoT) sensors and Building Management Systems (BMS) for data collection and analysis often outpacing security implementations, creating potential physical and digital vulnerabilities.

Asia Pacific is becoming a global hotspot for digital breaches, with a growing number of recent incidents involving bad actors compromising Operational Technology (OT) such as BMS, HVAC, and access controls via IT networks to lock down buildings, disrupt critical services, and cause physical damage.

The increasingly sophisticated nature of these threats may one day begin to impact owners' capacity to identify portfolio-wide vulnerabilities and secure their properties, potentially jeopardising both asset security and tenant operations.

Su-Fern Tan
Head of ESG
Pacific

Jonathan Hills
Senior Director
Asia Pacific Research

34%

of global cyber incidents occurred in Asia Pacific in 2024

13%

year-on-year rise in regional cyber incidents

17%

of Asia Pacific organisations sit in the cyber 'Exposed Zone'

Cybersecurity a Growing Concern for Regulators and Investors

Singapore's Cybersecurity Act and Australia's Security of Critical Infrastructure Act are examples of laws already reshaping obligations for tenants across commercial real estate, providing regulators with a platform to sharpen their focus on cyber risk. At the same time, cybersecurity is increasingly becoming a governance signal for investors.

This is because digital threats present major material risks to a company's stability, stakeholder trust, and resilience. Once treated purely as an IT issue, investors and regulators have come to view cyber resilience as a critical measure of corporate accountability.[1]

Corporate cybersecurity policies and programmes reflect how well an organisation manages key areas of governance, such as operational risk, data stewardship, and business continuity. Approaches to cybersecurity also contribute to social areas, such as tenant data privacy, employee safety systems, and community resilience.

[1] https://www.manageengine.com/log-management/cyber-security/cybersecurity-esg-for-every-board.html

What Types of Cybersecurity Threats Exist?

Cybersecurity vulnerabilities within commercial real estate exist in the technologies that run a building's day-to-day operations.[2] These include:

Building Management Systems (BMS): Building Management Systems (BMS): Software controlling heating, ventilation, air conditioning (HVAC), lighting, and elevators often are directly connected to IT networks or the open Internet and frequently lack basic security updates, leaving doors wide open to remote network takeovers. WiredScore's 2026 Global Insights report found that 75% of organisations globally are operating BMS's with known vulnerabilities, with just half of smart buildings performing annual assessments to mitigate these risks.[3]

OT and IT Network Convergence: Modern buildings connect physical facility equipment (OT) directly to corporate data networks (IT) or cloud environments. This can let attackers use a low-security device, such as an internet-connected security camera, as a springboard to infiltrate sensitive tenant databases. Approximately 50% of cyber incidents globally now occur in these systems.[4]

Physical-to-Kinetic Disruptions: Threat actors can weaponise infrastructure by disabling data centre chillers, shutting off hospital operating theatre power, or locking guests out of digital key systems.

Supply Chain Interconnectivity: Commercial facilities contain thousands of unmanaged IoT sensors from third-party vendors. This fragmented digital supply chain creates a multitude of unsecured internet-facing edge targets. With subcontractors, architects, maintenance vendors and other third-party providers having network access, a breach in their systems can ripple into an owners' building.

[2] Digital Risks in Buildings, RICS, June 2025.
[3] 2026 Wiredscore Insights, Wiredscore, January 2026
[4] 2026 Wiredscore Insights, Wiredscore, January 2026

Rising Cybersecurity Threats Impact Physical Infrastructure

Data show cybersecurity threats and incidents involving commercial real estate in Asia Pacific are increasing. The region is now a global leader in digital breaches, experiencing the largest number of global cyber incidents in 2024, representing a 13% increase from the prior year and accounting for 34% of the global total.[5]

Recent cybersecurity-related facility shutdowns in Asia Pacific underscore the severe real-world consequences of digital attacks targeting physical control systems and supply chains. Examples of digital breaches directly forcing physical infrastructure and operational lockdowns include:

- A major logistics and port operator in Australia suffered a data breach and network intrusion in November 2023.[6] To contain the threat and prevent further unauthorised network access, the firm disconnected its corporate network, resulting in a three-day shutdown of landside port operations in multiple cities.

- A Japanese media firm suffered a ransomware attack in June 2024.[7] After a network shutdown failed to stop hackers from remotely restarting servers, the company executed a physical infrastructure shutdown by cutting physical power cables within its data centre and temporarily closing its headquarters building.

- A major ransomware attack on Indonesia's central data centre facilities forced a widespread operational shutdown in summer 2024.[8] The incident paralysed over 280 essential government services, including disrupting immigration and airport check-in operations.

More recent breaches over the past 12 months indicate a shift toward targeting the construction supply chain and software that manages modern building environments. Recent incidents include:

- The Malaysia office of a global engineering and consultancy company was targeted by a ransomware group which claimed to have obtained engineering documents, financial files and confidential project data.[9] Stolen data reportedly included project drawings which could be used to create a digital blueprint for future physical or digital infiltrations of specific smart buildings.

- In 2026 Singapore's Cyber Security Agency (CSA) announced that all four of the country's telecoms companies had fallen victim to a cyber espionage campaign.[10] Hackers obtained persistent rootkit access, potentially creating a "kill switch" capability for entire metropolitan building networks.

- Hotels are emerging as high-value targets for hackers due to their reliance on BMS's for guest access and comfort, with major hospitality chains recently suffering severe ransomware attacks that paralysed operations.[11] During these attacks, hackers crippled backend booking platforms, room key encoders, and digital payment systems, leaving guests temporarily locked out of their rooms and forcing check-ins to be processed on paper. While these incidents occurred in the U.S., they caused consternation in the Asia Pacific hospitality sector by demonstrating how compromising a BMS can disrupt daily operations.

[5] 2025 Threat Intelligence Index, IBM, 2025.
[6] https://www.abc.net.au/news/2023-11-11/dp-world-australian-ports-cyber-security-incident/103094358
[7] https://www.rescana.com/post/kadokawa-corporation-and-niconico-cyberattack-june-2024-ransomware-breach-and-system-vulnerabilitie
[8] https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/
[9] https://botcrawl.com/meinhardt-group-data-breach/
[10] https://beeble.com/en/blog/singapore-exposes-major-cyber-espionage-campaign-targeting-all-four-telecom-operators
[11] https://asimily.com/blog/cyberattacks-hospitality-2023-2025/

How are Building Owners Preparing for Cyber Attacks?

Commercial real estate owners in Asia Pacific are relatively less prepared for cyber-attacks compared to their counterparts in North America and Europe.

Accenture's State of Cybersecurity Resilience 2025 report found that approximately 71% of Asia Pacific-based organisations fall into a so-called cybersecurity "Exposed Zone," lagging North America and Europe where mature cybersecurity postures—though still low globally—are statistically higher.[12]

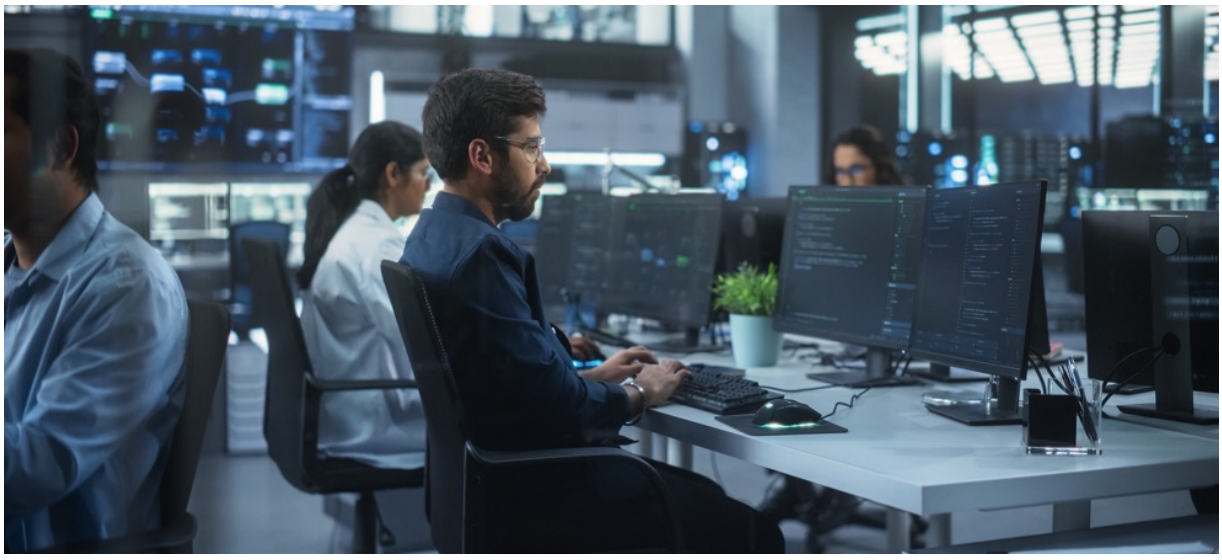
This vulnerability is being driven by the rapid adoption of IoT-connected smart buildings which is expanding the digital attack surface faster than physical security teams can implement protective measures.

Leading commercial real estate landlords in Asia Pacific have cybersecurity policies and practices in place. This is particularly the case among owners of high-grade premium assets, for which tenants often request the insertion of cybersecurity-related clauses into lease agreements together with a stipulation for regular testing to ensure properties are protected from potential breaches.

Most property owners retain a reactive approach, however, acting only after a breach occurs. The response often triggers a portfolio wide review but does not go further to strengthen protections. Around 69% of Asia Pacific business leaders acknowledge that it would take an actual, disruptive cyberattack to motivate their organisation to change their protocols.[13]

Implementing a robust cybersecurity strategy requires capital investment and ongoing management. This means defensive security spending is assigned lower priority than initiatives such as revenue-generating property upgrades.

Asia Pacific landlords' focus remains more on tenants' data protection than potential building hardware attacks. This may be because data breaches carry immediate legal liabilities, result in hefty fines, and can cause serious reputational damage. Property managers pay strict attention to vetting third-party vendors, however, who are required to have cybersecurity insurance and rigorous cybersecurity policies.



[12] State of Cybersecurity Resilience. Accenture. 2025.
[13] https://www.hsfkramer.com/insights/reports/2025/are-you-cyber-ready-apac

How Can Building Owners Confront Cyber Threats?

Many buildings are vulnerable to cyberattacks because cybersecurity is treated as an IT issue rather than a built environment one. This approach does not consider the critical convergence of digital and physical security. Modern buildings' reliance upon interconnected BMS for HVAC, access control, and elevators means a cyberattack is not just a data breach—it directly compromises occupant safety and energy efficiency, making it a fundamental corporate sustainability issue.

A cybersecurity policy is critical for addressing issues because it establishes the foundational rules, risk management frameworks, and incident response strategies needed to protect digital assets. Without it, organisations are highly vulnerable to preventable breaches and financial or reputational damage.

The first stage in devising a cybersecurity policy is compiling an inventory of all building systems to create an asset register. This enables property managers to gain a thorough understanding of all technologies and hardware in an individual property and their potential exposure to external threats.[14]

Property managers then compile a playbook on how various areas of cybersecurity are addressed across key hardware such as internet networks, building systems, landlord integration networks and the building's software system.

Other key elements include:

- Regular risk assessments and testing. This typically involves creating schedules of when cybersecurity assessments will be undertaken across the smart systems of a building on a regular basis, along with previous reports of cybersecurity assessments that have occurred over the past 12 months.

- Effective lifecycle management for hardware. This is essential, particularly when older legacy properties are involved. Building managers must have measures in place to address issues, such as when to replace older hardware and software and the extent to which such actions can mitigate risks.

- System recovery procedures.

What's Next for Building Cybersecurity?

Artificial Intelligence (AI) is set to play an increasingly prominent role in building cybersecurity in the coming years, both as a defence mechanism and an attack vector.

On the defensive front, AI-enabled systems can detect anomalies in a building's energy consumption or access patterns in real-time, halting automated attacks almost immediately.[15]

At the same time, however, generative AI is being deployed by adversaries to scale phishing and social engineering attacks, including impersonating leasing agents and tenants, designed to trick facility management or on-site staff into granting system access.[16]

[14] Cybersecurity: Fortifying Commercial Real Estate for a Digital World, CBRE Global Research, 2023.
[15] https://pmc.ncbi.nlm.nih.gov/articles/PMC12736962/
[16] https://www.mrisoftware.com/blog/ai-cybersecurity-in-proptech-addressing-privacy-and-technology-risk/

CBRE expects the future of building cybersecurity to shift from treating physical infrastructure and IT as separate domains to implementing holistic cyber-physical security, where all smart devices, HVAC systems, elevators, and access controls are treated as critical network endpoints. Integrating these systems will ensure compliance and safeguard communities.

Obtaining certification from providers such as WiredScore, which assesses and grades cybersecurity and data management in commercial and residential real estate, through its SmartScore certification, can help property owners independently benchmark their building infrastructure to ensure physical and digital networks are protected against cybercrime and unauthorised access.[17]

A property's level of digital resilience may one day be a commercial differentiator. Government departments and tenants in industries handling sensitive information, such as financial services and life sciences, are already requiring tighter building cybersecurity to ensure regulatory compliance.

This could lead to the emergence of "cybersecurity stranded assets"—a scenario where a property's digital infrastructure, OT and legacy systems prematurely lose their economic value and appeal to tenants due to security obsolescence, unpatchable vulnerabilities, or the failure to meet modern regulatory and data protection standards.

With a holistic sustainability strategy that incorporates cyber risks, commercial real estate landlords can create an offering that is **smart, sustainable** and **secure**.

[17] https://wiredscore.com/certify-a-building/smartscore/

Contacts

Corrado Forcellati
Senior Director
ESG Consulting & Sustainability Services, Asia Pacific
Head of Paia FROM CBRE
corrado.forcellati@cbre.com

Su-Fern Tan
Head of ESG
Pacific
su-fern.tan@cbre.com

Jonathan Hills
Senior Director
Asia Pacific Research
jonathan.hills@cbre.com.hk