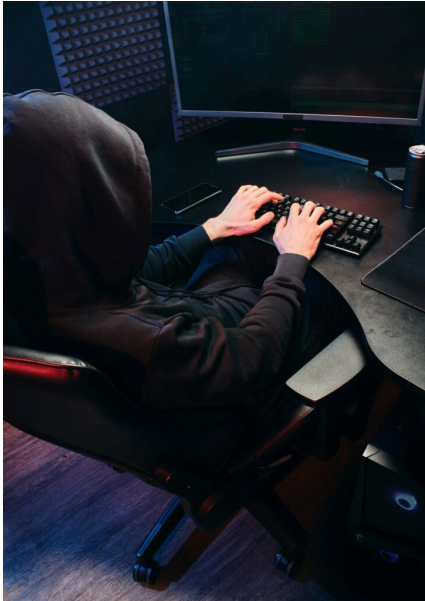# UK businesses risk sleepwalking into cyber attacks unless immediate preventative action is taken, say RICS

22 hours ago

Owners, managers and occupiers of commercial buildings neglecting to take responsibility for digital security of their properties face increasingly prevalent and far-reaching consequences threatening the safety, resilience and sustainability of their assets and operations.

A new practice information paper published by the Royal Institution of Chartered Surveyors (RICS) highlights the rapidly increasing and diverse threat of digital risks to commercial properties worldwide.

With cybercriminals becoming more sophisticated and the range of potential cyber threats to buildings expanding, attacks on critical infrastructure and data breaches are becoming more common. Augmented by the rising capability of AI and the pace of change, the threat to cyber security is set to accelerate further.

In a startling illustration of the growing prevalence of digital risk, a survey undertaken by RICS of Facilities Managers, service providers and FM consultancies revealed that 27% of respondents said their building had been the victim of a cyber attack in the last 12 months. This represents a significant increase of 11% on the previous year, when 16% of respondents had experienced such an attack.

The paper identifies operational technology such as building management systems, CCTV networks, Internet of Things (IoT) devices and access control systems as risk areas. This covers everything from automated lighting and HVAC systems to advanced security protocols and energy management.

It also notes concerns that some buildings use outdated operating systems (OS). A building opened as

recently as 2013 could conceivably use Windows 7; an OS that hasn't received security updates from Microsoft in over five years.

Beyond the direct impact on the operation of a building and its occupiers (users), the paper examines additional considerations such as Insurance, Reputation, Building Value and AI.

Critically, the paper sets out three 5-point action plans for owners, managers and occupiers of buildings; professional industry bodies; and Governments to follow to mitigate risks and safeguard their properties against attacks (see notes to editors).

RICS Head of Property Practice, Paul Bagust, said: "Buildings are no longer just bricks and mortar, they have evolved into smart, interconnected digital environments embracing increasingly sophisticated and ever-evolving technologies to enhance occupier experience.

"This has led to increasing data being collected and used to inform decision making; at the property manager, building user, occupier and owner levels. However, while these technologies bring many benefits, from efficiency gains and reduced negative impacts on the planet, they also create multiple risks and vulnerabilities which can be exploited by those looking to cause disruption.

"It is inconceivable to imagine a world where technology will not continue to pose a growing risk to a building's operation, and it is equally impossible to consider that the management of digital risks will not be needed as an imperative measure to safeguard the future of a building and prevent systems from being compromised.

"I implore building professionals to read the paper and act now. Failure to identify these growing digital challenges and incorporate security countermeasures risks businesses sleepwalking into cyberattacks."