FMBusinessDaily

The crucial role of cyber security in modern FM

1 year ago

Insight from Corps Security executive director Mike Bluestone and Toto Solutions director Katie Barlow

In today's increasingly digital world, the integration of technology into facilities management has become commonplace, offering efficiency and convenience. However, this reliance on digital systems also brings with it significant cyber security risks that can no longer be ignored.

The risks, threats, and vulnerabilities such as hacking, phishing, and the introduction of malware, that accompany digital systems has inevitably impacted on the design and content of corporate security strategies, policies, and procedures. Across the whole spectrum of corporate management, from the C-suite down, the emphasis is now on a convergence of physical and cyber security measures, the driver being the increasing nature of risk and threats to UK corporations and businesses posed by hostile state actors, namely Russia, Iran, China, and North Korea, as well as those emanating from organised and opportunist criminal sources. Over the past decade Government has recognised the seriousness of these risks and threats, and working in tandem with the professional security sector, it has been promoting via the Cabinet Office, the need for businesses to not just apply a converged approach to security risk management, but also to buy-in to the concept of 'Organisational Resilience'. In this way the emphasis is not just on managing threats and attacks (of whatever kind) but also enabling businesses to survive, recover, and go on to prosper and grow.

In facilities management, the integration of IT and OT in building technology systems has introduced a number of cyber security risks. Modern facilities rely heavily on interconnected devices, sensors, and controllers for efficient monitoring and control, particularly in HVAC and building automation systems. While these advancements improve energy management and indoor environments, they also create

vulnerabilities. Cyber threats targeting these systems can lead to data breaches, unauthorised access, system manipulation, and even physical damage to building infrastructure. HVAC and automation systems, controlling crucial building functions like temperature and lighting, are enticing targets for cybercriminals seeking access to organisational data. Vulnerabilities in software, hardware, and communication protocols pose significant risks, potentially resulting in discomfort for occupants and compromising sensitive information such as personnel and financial data.

A cyber-attack on facilities management systems could trigger a series of detrimental consequences. Operations may come to a standstill as essential systems controlling lighting and access to facilities face disruptions. The breach of sensitive data, such as building layouts and employee information, could jeopardise numerous individuals. This, coupled with substantial financial losses, reputational harm, and regulatory compliance issues, underscores the severity of a potential attack.

Facilities managers must therefore adopt a multifaceted and converged approach to security, integrating both physical and cyber elements to ensure comprehensive protection.

They should do this by applying a layered approach to security planning and the implementing appropriate measures. Achieving complete buy-in by all corporate personnel is a crucial element of this approach.

Security strategies must provide not just for physical and electronic preventative and response solutions, but also for delivering security awareness training for all personnel, along with strict operating procedures and protocols, which capture third party partners, and other stakeholders such as contractors. There must be no gaps in the ‘security system’, and the aim must be to instil a robust and resilient corporate security culture in which everyone has a role to play within. As the saying goes, “you are only as strong as your weakest link,” highlighting the importance of a cohesive and collaborative approach to security across all levels of an organisation.

To gain a better understanding of your security, start by conducting a security review, this will identify and recognise risk across your organisation’s people, processes, and technology. From this assessment, build a roadmap of remediations to improve your security maturity and create business resilience. This proactive approach ensures that future investments made in security are risk-informed and provide appropriate mitigation against potential threats.

As facilities management becomes increasingly reliant on digital systems, the need for robust cyber security measures has never been greater. By adopting a converged approach that integrates physical and cyber elements, organisations can better protect themselves against evolving threats.