# SMART BUILDING SECURITY

**Mirel Sehic** *discusses what can be done to plug the gaps in smart building cyber security*

**Pervasive connectivity is improving our built environment; technologies such as edge and cloud computing, machine-to-machine (M2M) communication and artificial intelligence (AI) are driving exponential change. As a result, we are living and working in smarter, more proactive, service-driven environments, which are being networked into cognitive communities of AI-enabled buildings. At their heart is an information-rich web of smart devices, sensors and real-time data collection that is shaping how we interact with our surroundings.**

Although the convergence of intelligent technologies and physical environments has significantly improved the operation and performance of networked buildings, this move to widespread digitisation has also exposed previously unidentified security vulnerabilities and increased points of attack.

For instance, the capacity to analyse data from physical devices in real-time to support immediate and even predictive decisions often provides an unprecedented advantage over traditional capabilities. Yet these abilities are often accompanied by heightened cyber security risks if not reviewed, remediated and supported correctly. It is therefore little wonder that these systems are starting to attract the attention of cyber criminals.

## AN ATTACK ON AN OT ENVIRONMENT CAN HAVE CONSEQUENCES BEYOND JUST FINANCIAL LOSS

To build a strong cyber security ecosystem, it is essential to have an understanding of the attacker's intentions as well as the range of common cyber risk scenarios. The top three goals are financial gain, disruption of service and theft of personally identifiable information and company intellectual property. The types of risk scenarios, however, are more fluid due to changes in the underlying technology and an increase in network integration.

The last decade has witnessed a growth in investment in cyber security for information technology (IT) systems, partly in response to some high-profile attacks, which have caused hundreds of millions of dollars of damage worldwide. Consequently, governments and businesses of all sizes are committing time and money to a range of initiatives aimed at thwarting even the most determined cyber criminals.

The good news is that cyber security responsiveness is now commonly integrated into IT planning and day-to-day operational thinking. However, the built environments that house IT systems aren't always afforded the same levels of protection. The evolution of Internet of Things (IoT) connectivity and large-scale digital integration have the potential to undo all the good work by presenting would-be attackers with new, low security points of access.

## HEART OF THE MATTER

The heart of the problem is operations technology (OT), which has historically not needed a full suite of digital armour as it has traditionally worked inside discrete networks. This is increasingly not the case as a result of a burgeoning use of new technology to improve business operations. As more internet-connected devices are being incorporated into building operations, facility managers, along with IT and OT professionals, need to collaborate to create and manage holistic cyber security policies and procedures to ensure the optimum levels of protection.

This, in turn, is raising a new challenge for businesses and facility managers – the need to understand how their digitisation strategies are impacting the cyber security status of their building portfolios. And there's no time to lose as the threat landscape is rapidly evolving. It is, therefore, essential to have a firm grasp of the potential cyber security vulnerabilities and risks associated with implementing new technologies and the steps that need to be taken to instigate the appropriate defences against cyber attacks.

The more complex the system, the more difficult the diagnosis of the potential risks. On the other hand, older parts of OT networks often have little or no protection at all. As such, facility managers need to devise top-to-toe risk management strategies that address weaknesses in both complicated new technologies and legacy systems.

Incorporating IT capabilities, such as big data analytics and IoT connectivity, across OT environments can vastly improve productivity. Multiple proprietary systems can be easily centralised and automated, which further helps optimise building performance. However, the implementation of new technologies and a greater number of entry points increases the possibility of cyber attacks and malicious activity, especially around unauthorised access to controls and security systems. The application of new technologies, therefore, needs to be accompanied by a concomitant rollout of suitable protection.

A raised awareness and understanding of cyber security risks in OT systems is vital in order to ensure that decision makers are better able to make smart purchasing decisions, perform targeted OT security controls, train staff in effective policy actions and ensure improved cyber resilience.

While loss of personal data can have financial costs, an attack on an OT environment can have consequences beyond just financial loss – including prolonged outages of critical services, environmental damage and a danger to personal safety. There's also the threat of a third party gaining unauthorised access to internet-connected physical security systems.

There have been an increasing number of attacks on the manufacturing industry, critical Government infrastructure such as dams, public transport and hospital networks. The most recent Notifiable Data Breaches report indicates that violations have occurred more regularly month to month, with the health sector reporting the most cyber attacks out of any other sector. Worse still, 61 percent of these attacks were identified as malicious or criminal.

Make no mistake, there are highly skilled and motivated criminals actively targeting networks to find ways to exploit the security weaknesses in the OT environment, control systems and critical infrastructure. Understanding how an attacker can gain access to a system, including the various attack techniques, is an important step towards mitigating the risks and will help organisations keep on top of the threats that exist in their own networks.

Having a cyber security strategy in place is critical; readiness isn't optional. This starts with employee training and awareness but facility managers also need to identify which assets need safeguarding, the types of likely threats and the rules and controls needed to protect against them.

## CLEARLY DEFINED STEPS

Developing, reviewing and maintaining policies and procedures is paramount, including guidelines for password use and renewal, the handling of sensitive data and the use of removable devices, to name just a few. Having employees follow clearly defined steps really can be the difference between a cyber incident being a slight hiccup rather than a total disaster.

A thorough risk assessment will also be extremely useful. Starting with an asset inventory enables an organisation to identify what is connected to a network; establish a baseline for network traffic to help identify existing gaps and potential security vulnerabilities tied to the OT environment; and assist in formulating more effective protection methods. These findings can then be leveraged to create a cyber security strategy that is specific and detailed.

In reality, industries and organisations differ in their acceptance of cyber security risk, which is sometimes referred to as 'risk appetite'. Having a lower risk appetite leads to a high focus on cyber security, while a higher risk appetite translates into less rigorous cyber security practices. The reality is,

**Facility managers need to collaborate with IT professionals to create holistic cyber security policies for optimum protection**

however, that every business is in danger of attack. The primary focus for cyber criminals includes critical operators such as hospitals, data centres, government buildings, airports and banking. However, past experience shows that their targets also include premium commercial buildings, for example high-end offices, upmarket hospitality and retailers of all sizes.

## THE MOVE TO WIDESPREAD DIGITISATION HAS EXPOSED UNIDENTIFIED SECURITY VULNERABILITIES

Preparedness is unavoidable; thinking "it won't happen to me" isn't a defence. As with insurance, the better your cyber security, the better your protection and the quicker your business will bounce back. Cyber threats are constantly evolving and with OT systems being targeted more each day, your facilities need to keep pace. Cyber criminals are finding new ways to bypass security and access data, so it's crucial that all stakeholders work together to raise the bar to protect their investments. A proactive approach to security will produce the best results, now and in the long term.

And it won't be getting any easier; the cyber criminals will see to that, so the longer you put off acting, the harder it will become to secure your built environment. The convergence of OT and IT systems is also gaining pace, so it is essential that organisations are aware today of the risks across their OT environments and enhance their security provision to reduce the likelihood of successful cyber attacks, now. The bottom line is that the landscape of cyber security is changing and evolving in tandem with technological advancements. Facility managers are key decision makers in how to prevent and respond to security issues. As a result, it's important they keep up to date with the latest insights and protection methods.

Developing a mature cyber-smart strategy involves a continuous assessment of internal procedures, employee awareness programmes and the introduction of appropriate applications, all of which are specific to a set of defined organisational requirements. This can be challenging and a drain on resources if not properly handled. Facility managers should therefore always work with specialist suppliers that have the knowledge and experience to help formulate and install the most appropriate cyber security systems ●

**Mirel Sehic** is the Global Director Cybersecurity for Honeywell Building Solutions. Mirel is responsible for increasing awareness and steering key stakeholders toward Cyber Security industry best practice and increased resilience.

**It is vital to ensure decisions target OT security controls, to train staff in effective policy actions and ensure improved cyber resilience**