the SOURCE
powered by CoreNet Global

Is your smart building an easy target for hackers?

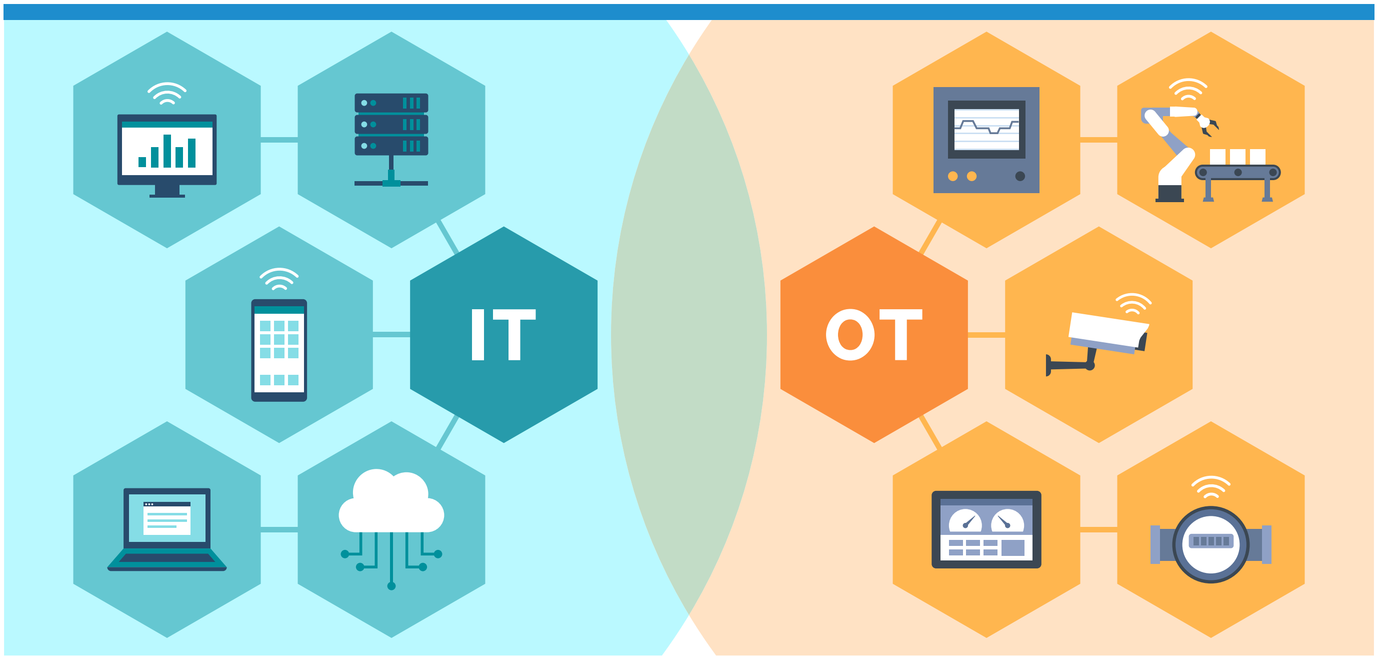
BY COLEMAN WOLF | DECEMBER 2023

The latest building system technologies being adopted bring many benefits in terms of operational efficiencies, reduced environmental impact, and enhanced occupant experience. But these systems also introduce new vulnerabilities and present a much more tempting target for malicious actors seeking to launch cyberattacks. So do the benefits outweigh the risks, and how should potential vulnerabilities be addressed?

The introduction of intelligent buildings

Advancements in smart building technology have transformed the day-to-day management of buildings. Nearly every aspect of a facility can now be controlled remotely through a series of interconnected sensors and actuators via computers. Operational technology (OT) systems such as building automation systems (BAS), air quality monitoring, elevators, building access control, video surveillance, and more can now be monitored and controlled remotely. Today more than ever, building owners, operators, and tenants expect their facilities to be safe, secure, and more productive while also enhancing occupant experiences through the optimization of space, systems, and services.

We are currently emerging into an evolving, post-pandemic workplace that demands greater monitoring and control of indoor air quality (IAQ), detailed



awareness of occupancy as people interact with the different spaces, and enhanced control of facility access. Furthermore, these modern intelligent building systems also help prepare properties to address new health threats as well as future environmental sustainability requirements through increased data collection, analysis, and control.

The age of the intelligent building is upon us, and as intelligent-building platforms continue to grow and evolve, so too will the frequency and nature of the cyberattacks we can expect to see targeting these systems.

Where to look for unexpected vulnerabilities

Early building control systems were not typically built with strong security in mind. They tended to be self-contained systems isolated from external access, and it would take some type of physical contact to compromise them. A workstation login and password often were all that was really needed. With modern buildings increasingly being connected with the outside world, exposure to those systems has grown exponentially, leading to an increased danger of cyberattacks.

However, the potential impact on building-control systems like lighting, lobby monitor displays, thermostats, and other less obvious targets may not always be recognized. While the direct effect on those systems may be relatively minor, the larger ramifications may be much more serious, and the compromise of those devices may not be the ultimate goal of an attacker. The fact that those devices are easy to connect to and likely have vulnerabilities that are easy to exploit makes them valuable initial steps for an attacker to gain further access to a network to reach other targets. If an attacker finds that other entry points to a network are well secured, they will look to alternate entry points; with OT systems increasingly connected to networks, those attackers are finding that they often provide a path with much easier access.

The attacker's goals may be theft of valuable information, but it could also be some sort of disruption of systems or operations. With IT systems, this disruption may be in the form of deleted or modified data or denial-of-service, or it could be ransomware, whereby data is encrypted until the victim pays a ransom to the attacker. With OT systems, the nature of these disruptions can be significantly more severe. Imagine the potential damage resulting from loss of critical OT systems in a hospital, or power at a casino, or cooling at a data center. And for many systems, availability and integrity is important to the health and safety of personnel, adding further potential risks.

As an example of a recently reported cyberattack, hackers were able to gain access to an unnamed Las Vegas casino database via an internet-connected “smart thermometer” used to maintain a high-tech aquarium in its lobby. The breach of this seemingly innocuous device allowed the cybercriminals to bypass security measures and navigate to other systems to steal 10 gigabytes of information from a “high roller” database. The unusual heist highlights the vulnerability of Internet-of-Things (IoT) devices. According to IOT Analytics, the number of connected IoT gadgets is expected to grow 18 percent this year to 14.4 billion devices globally. The trend also underscores the increased vulnerabilities property owners and cybersecurity professionals face.

Limiting access and opportunity

While data theft such as theft of financial or other personal information often gets the most attention, there are other threats that can be just as costly and potentially more dangerous. The reliability of systems that control and monitor facility operations is also needed. The continual collection of information by connected devices about our individual environments and activities could also seriously impact how business and personal decisions are made. Fortunately, we are starting to see better protection measures, although there is still a long way to go.

While different systems have different requirements, the following are some basic security recommendations to better protect your building and operations:

- Segregate systems on separate networks wherever possible.
- Actively manage system accounts, including unique and strong passwords for each component and controlling system account assignment and privileges.
- Create a program to manage software and firmware patches and updates to reduce risk exposure.
- Document your systems thoroughly. Too often a company doesn’t have accurate system information and you can’t manage what you don’t know.
- Perform cybersecurity testing of your systems on a routine basis. The systems themselves are not static and new vulnerabilities are discovered every day, so it is important to stay current.

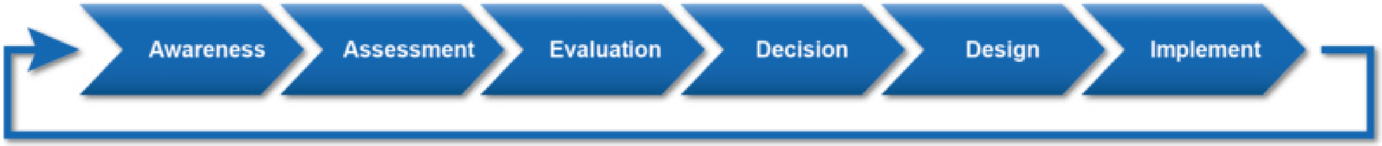
Creating a cybersecurity action plan

As information technology (IT) and OT systems become increasingly intertwined, it is clear a unified approach to security is needed. But the frequent question asked is “who should manage cybersecurity for these systems?”

> *(M)any companies are beginning to understand that both OT and IT systems need to be managed holistically under the overall goal of risk management. Communication is fundamental to successful convergence.*

According to an ASIS survey, the biggest obstacle slowing organizations to adapt to combined systems revolve around people issues. Physical security departments are often set in a history of siloed traditions and functions. Personnel are often hesitant to give up or share control of what they consider to be core competencies, including people management, intelligence, and investigations. IT professionals can be equally rooted in their own routines built around the latest technology, system innovations, and cyberthreats.

Loss of authority, status, control, or staff are equally feared by both groups and this often results in a lack of communication. It often leads to the two sides



not recognizing security gaps or, worse, assuming the other is addressing specific concerns. Despite these hesitations, many companies are beginning to understand that both OT and IT systems need to be managed holistically under the overall goal of risk management. Communication is fundamental to successful convergence.

In many instances, IT is the gatekeeper to all devices allowed on a company's network. Bringing IT and OT stakeholders together early in the project's design-development process – preferably during initial master-planning phases – can help avoid conflicts and eliminate implementation-schedule delays. While it is common for organizations to put their intelligent building system and individual OT system components on the company's enterprise network, it comes with inherent cybersecurity risk. If devices are not thoroughly vetted, tested, and approved by IT, chances are they will not be allowed to connect, potentially leading to missed expectations and lost operational opportunities.

In the end, being more integrated and interconnected does not inherently mean your facility is more vulnerable, but it does make the security considerations more complex. In fact, the additional systems can actually make building automation systems safer if they provide more detailed intelligence that allow operations personnel to respond to a cyberattack more accurately and efficiently. And if the integration of these devices and systems drives more and better engagement between stakeholders, we can expect to see overall better security, improved operations, reduced utility consumption, and increased occupant comfort, delivering on the promise of the intelligent building.

Cybersecurity is a journey, not a destination.

Implementing a successful cybersecurity risk management plan is a cycle that begins with awareness and works through implementation before starting over again. In addition to engaging a qualified third-party expert to help guide you along the way as well as conduct independent assessments, there are two specific steps every company should take now:

1. **Get your IT and OT teams together now**
   - Obtain support from top down to address organizational risks.
   - Work jointly to identify gaps in security measures.
   - Develop a unified cybersecurity policy and mitigation strategies.
2. **Know your security posture**
   - Document your systems ("You can't manage what you don't know").
   - Assess vulnerabilities and risks for your systems and existing protective security measures.
   - Conduct regular check-ups to reassess posture and assess corrective measures.

Coleman Wolf, CPP, CISSP, SmartScore AP, is studio leader and senior security consultant at Stantec.

Published by CoreNet Global. Articles may not be reprinted without written permission from the editor, Tim Venable. For reprint permission, please contact tvenable@corenetglobal.org.

CoreNet Global is an opinion leader in corporate real estate, workplace and infrastructure management. Enhance your knowledge with resources like research papers, exclusive member survey reports and presentations from top speakers on hot industry topics. Members of CoreNet Global benefit from a wealth of research knowledge and resources – find out more at www.corenetglobal.org.