5 Steps to Reduce Cyberattack Threats

The cyber threat landscape is expanding, and it's important for every facility professional to be on guard against potential breaches. Keep your organization's assets safe and put these five tips into practice today.

BUILDINGS®

UNDERSTAND POTENTIAL CONSEQUENCES

Cyber attackers who gain access to a building's control systems can accomplish anything from hijacking your elevators to disabling your power supply or even tampering with your lighting systems. You may have to evacuate the building, and the downtime can cause significant financial losses for your company. Bad actors can also put your occupants in danger by manipulating building temperatures, disabling fire alarms, and more.

However, it's important to know that cybercriminals may not even be interested in the building systems themselves—your building systems may just be an easy entry point into your corporate IT network. From there, they can cause data breaches and cost your organization a lot of money.

5 STEPS TO REDUCE CYBER THREATS

There are a handful of strategies you can implement to improve cybersecurity at your organization—and you can start today.

- **Collaborate with IT to secure your building's networks.** This isn't just an IT issue—facilities needs to be involved too, and the two departments should collaborate frequently and maintain open communication. Are you planning to introduce any new operational technologies? Partner with IT for the rollout. Both departments should also stay up to date on the latest cyberthreats.

- **See which systems are exposed and how.** Know what your system is showing the world. Look for any systems that could be unprotected and close those loopholes right away. For example, does your Wi-Fi extend outside the building? That can increase the risk of unauthorized access, leading to data breaches.

- **Audit and update your device inventory.** Do you know what you have and how it's connected? This can be a major undertaking for today's connected buildings, but it's important.

- **Control and update remote access.** It's common for service techs and vendors to be able to log into your systems so they can diagnose problems and make adjustments—but many technicians will share a common username and password, which is a problem because you'll never know exactly who's accessing your network. Take back your access control and insist on separate login information. If someone leaves your organization, voluntarily or otherwise, immediately revoke their username and password.

- **Train your staff.** Human error can allow cybercriminals to wreak havoc on your systems. Your whole organization, including your FM staff, needs to be trained on how to recognize red flags and respond to cyberthreats.