The Internet of Things Is Here

Property owners should secure their buildings' smart technology.

By Valerie M. Sargent / *Multifamily Broadband Council*

Multifamily owners are thinking about what the internet of things (IoT) means to them and wondering how they can leverage that technology for energy management, smart appliances and other services. For some, the IoT promises operational savings. For others, it means enhanced services, such as proximity or location-based services. Regardless of the goal, ensure that you protect your network, community and residents.

That internet-enabled thermostat looks cute and innocent, poised there on the wall. It sits there quietly, with its sophisticated good looks and ease of programming, set to keep the temperature in that oh-so-perfect range. What could possibly go wrong?

Depending on how you connect and manage that device, a *lot* could go wrong. If you aren't careful with planning and installation, that connected thermostat (or any similar networked device) could bring down an entire network. Each low-powered device provides an entry point to the network that can be difficult to secure. These magical places are where the hackers go.

Zigbee, Z-Wave, Bluetooth Low Energy and Wi-Fi technologies are all accessible over the air, so a network becomes easier to hack into through these new entry points. If Mr. Hacker gets into a smart thermostat, what happens from there? What happens is that he can get into other devices and home computers and steal personal data, creating all kinds of havoc. The network itself may cease to function, internet service can be interrupted or mission-critical networked services, such as security, access control and energy management, can be disrupted. Yikes!

Knowing this, should property owners even consider the addition of smart technology? This is a classic risk-reward decision. Are the rewards of deploying IoT-based solutions worth the risk? Overwhelmingly, yes – as long as you consider the security-related issues first.

PROTECTING THE NETWORK

Fear not – help is on the way! Technology exists today to keep communities and residents safe from those who may try to harm a network. Think of network security as locks on a door – door locks will work *if* you actually put them on a door. The same is true of security measures to protect devices installed in apartments.

To start, consider pushing security out to the edge of the network if possible, utilizing the computing resources of devices such as wireless access points, switches and gateways to stop attacks close to the point of entry.

A gateway is a great place to provide security. The cute little thermostat is actually a dumb device. Only the data makes it smart, and predetermined settings can help the gateway manage security by using conditions and data to differentiate normal from potentially rogue activity.

Say, for example, the thermostat's network address begins a Transmission Control Protocol session. This strange behavior would alert network security, which could shut down or block the thermostat to manage the problem. The software defines what "acting strangely" means.

Similar measures can be put in place with occupancy sensors, heat sensors, wireless door locks, submeters, smart appliances – anything that fits into that IoT.

Next, select only vendors that are savvy about security. Make sure to hire an integrator or a managed service provider well versed in providing proper security functions. Ensure that the company understands security and how to deploy it. If a company says it can install smart devices but then plans to walk away afterward, you could end up with a problem. Don't buy anything from a company that doesn't know how to secure it.

Ask potential service providers what steps they will take to secure the network regarding IoT devices. Request examples that demonstrate their success in implementing network security for smart devices. If a provider tells you not to worry about it, look for other providers until you find a company that says, "We take security very seriously. Here are the steps we take to secure the network …"

Security risks don't need to happen to you. Smart owners buy smart technology that has even smarter security standards. Interview vendors. Ask the right questions. And start at the edge of the network. ❖

Valerie M. Sargent is a multifamily speaker, trainer and executive consultant, and she serves as the executive director of the Multifamily Broadband Council. Contact her at vsargent@mfbroadband.org or 949-274-3434. For more information, visit www.mfbroadband.org or www.valeriemsargent.com. Dean Compoginis, MBC Tech Committee member and head of hospitality and MDU solutions in the Americas for Ruckus Networks, contributed to this article.