IP addresses plays a role in your firm's security. This obviously includes mobile devices, but it may also include copiers, printers, thermostats, televisions, motion ...

Jim Boomer • May. 21, 2018

Last year, the Pew Research Center and Elon University's Imagining the Internet Center conducted a poll of experts to ask how attacks and ransomware concerns would influence the spread of connectivity, i.e., the "Internet of Things" (IoT). Of the

1,201 respondents, only 15 percent said they would disconnect, while 85 percent

conserve energy when they sense the last employee has gone home for the evening. And of course, everyone is carrying a smartphone or tablet both at home and at work.

All of this connectivity is convenient. It makes our lives easier and enables us to work from anywhere in the world as efficiently as we can work from the office, but as our home and work lives become more integrated, firms must give some consideration to the potential security trade-offs.

Any device that communicates and can be accessed via the internet based upon its IP addresses plays a role in your firm's security. This obviously includes mobile devices, but it may also include copiers, printers, thermostats, televisions, motion detection systems, fitness trackers and even smart trash cans (yes, that is a real product).

All these devices create access points and pose a security risk simply because more and more attacks on companies begin with individual employees. For example, if an employee's personal device is infected with malware or a virus, it can wreak havoc when that device connects to the company network. Depending on the device, an IoT device could be used to spy on you, steal your data or track the location of you and your employees.

The majority of these devices cannot be integrated into the conventional methods companies use to protect themselves against internet-based attacks, but there are steps you can take to monitor and secure the new data traffic on your network.

Consider the risk vs. reward

First, consider whether connecting a particular device will be a large enough benefit to be worth the risk. If the device is helpful, it may be worth the risk. On the other

hand, if it serves little purpose beyond its novelty, it may be best to leave it

Set up guest networking

When an outside associate, contractor or client visits your office, it can be convenient to offer wireless access. But don't just allow access to your existing Wi-Fi network. Use a router that supports guest networking so you can keep potentially risky devices off of your main network and protect its contents.

Educate employees and establish guidelines

It's easy for an employee to bring a device to work and connect it to the company network without considering the potential security risks. Many employees are just unaware of how their online behavior can place the firm at risk of data loss or breach. A robust security framework and educated employees – whether in the office, at home, or on the road – are critical to the healthy integration of the IoT and your firm. Establish guidelines for devices and define which ones are permitted on the company network.

Set effective password policies

Make sure passwords are strong and not reused between devices and accounts. This will help ensure that even if one account is compromised, access to the rest of your programs would require a different set of credentials.

The IoT allows people to sync to-do lists, access work files and answer email from co-workers and clients while traveling or at home, but it also introduces additional complexity for security. It doesn't need to be scary, but it's something your firm absolutely must consider and address.