Preventative MEASURES

DOES YOUR COMPANY KNOW HOW TO SECURE ITS IOT DEVICES?

WRITTEN BY **PEGGY KEENE**

AS THE INTERNET OF THINGS, or IoT, has made itself increasingly relevant across all industries, smart devices have become especially common in the workplace. As a result, privacy experts across the nation have noted a steep rise in cyberattacks on IoT devices as more and more smart devices are being used in industries that are relatively new to using IoT connectivity.

The Popularity of IoT Use Has Made It a Target for Hackers

Every day IoT is used in new and exciting ways. Whether it is a new industry finally "coming online" with IoT or an already established IoT industry finding a new channel to use the technology, it is clear that IoT is here to stay. IoT refers to the technology that allows for smart devices to stay "online" indefinitely while being able to receive, track, and send data wirelessly. These devices can be used to monitor everything from a patient's blood glucose levels to a satellite's uptime. While an industry's need for IoT devices may vary, the use of IoT devices is steadily increasing across the board. For example, IoT devices have become incredibly popular in health care. Just earlier this year, one health system in southwest Missouri disclosed that they extensively use more than 17,000 IoT-connected devices in the day-to-day management of their services.

But as IoT technology becomes more widely accepted, it has also become a more high-profile target for hackers. Such a problem is compounded by the fact that there are so many different manufacturers of IoT devices as so many companies want to cash in on IoT's popularity. This makes it harder to ensure that consumer devices have adequate protection in place against hackers and cyberattacks.

Tips for Securing IoT From Hackers

First, above all, secure your company's network. A company or system's network is the foundation to all its technology transactions. Securing a company's network can include multiple steps, such as installing a firewall, maintaining proper firmware, pushing regular updates to devices, having antivirus and anti-malware software on all devices, and limiting activity on company devices to pre-approved activities.

The second step is to have a strong understanding of what kind of communications the company's devices should be making. When experts speak of "communications," they are not referring to communication like email but to the dialogue between devices that occurs for IoT devices to function. Understanding this and training employees on what kind of use is permitted on their devices can help IT recognize when unauthorized access, i.e., hacking, is occurring.

Lastly, if budget permits, experts stress that company-issued devices should be from the same company, of the same model, and run the same software. This streamlines the process for IT when updates or patches must be pushed to the devices, and it can also make it easier for companies to train their employees.

Key Takeaways on Securing IoT Devices From Hackers

The hacking of IoT devices has become a real concern as more and more industries begin to use IoT technology. To deter hacking, experts suggest several preventative measures that include:

- Limiting the use of company-issued devices to approved activities only;
- Ensuring that all the devices used by the company are of the same model, manufacturer, and version; and
- Using safeguards such as antivirus software, anti-malware software, and firewalls. **TBJ**

This article was originally published on the Klemchuk Intellectual Property Trends blog and has been edited and reprinted with permission.

PEGGY KEENE
is of counsel to Klemchuk. Her practice focuses on intellectual property and internet law, e-commerce, and data privacy. Keene has also served as in-house counsel in the telecommunications industry.