CAPINTECH

Checklist of Controls to Secure Internet of Things (IoT) Devices

Before evaluating cybersecurity controls, you must **inventory all IoT devices** that are in your environment. An IoT device is anything that connects to the Internet. While some individuals consider network equipment, like firewalls and routers, IoT devices, these are often managed well. For purposes of this checklist, we will focus on non-standard devices that are often overlooked.

Common IoT devices include the following. Which of these connected devices are present in your environment?

- □ Smart TVs
- □ Amazon Echo
- □ Thermostats
- □ HVAC systems
- □ Environmental monitoring system
- □ Coffee makers
- □ Card systems
- □ Multi-function printers
- □ Copiers and scanners
- □ Fish tanks
- □ Smart refrigerators
- □ Alarm system
- □ Doorbells
- □ Light switches
- □ Smoke alarms
- □ Cameras
- □ DVR systems

Document these devices in your hardware inventory and on your network diagram. Inventorying these devices is critical for asset management, lifecycle processes, and system hardening. Depicting how these systems interact with other devices is also essential to identify data flow and aid in investigation of potential issues and breaches.

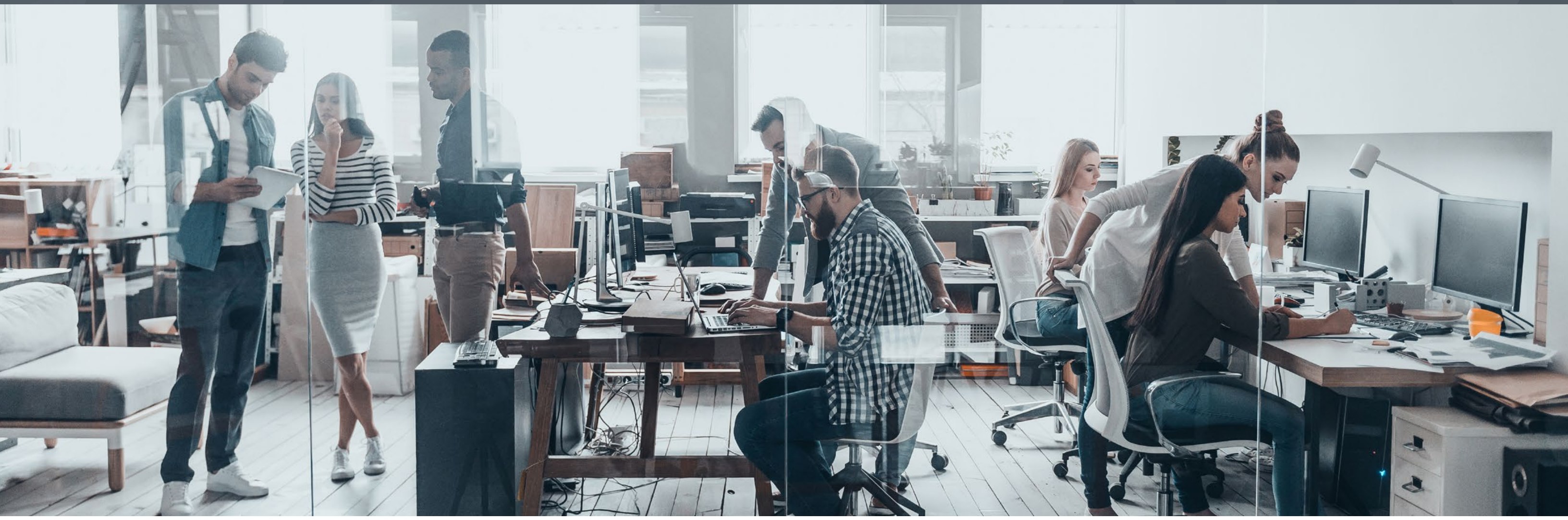
Once you've identified all systems, evaluate and implement controls. All devices may not support the same security features. However, implementing layers of control will minimize the risk that these devices are exploited or used to gain a foothold to the network.

Authentication

- □ Change default passwords initially and annually thereafter
- □ Change administrative passwords whenever employees who had access to the passwords leave your organization
- □ Enable strong passwords, lockout settings, and multi-factor authentication
- □ Store administrative passwords in a secure, limited-access location
- □ Add each device to your onboarding and termination processes to ensure access rights are adjusted in a timely manner upon employee turnover or change in job function
- □ Create individual user accounts to replace any shared accounts
- □ Review all access to devices annually to ensure rights remain restricted

Device Security

- □ Configure devices for centralized management via an existing device management solution (if the solution supports these non-standard devices)
- □ Evaluate and apply security updates promptly
- □ Connect devices to a guest wireless network that is segmented from the data network or isolate less secure/riskier devices via VLANs, DMZ, etc.
- □ Disable unnecessary features
- □ Evaluate data and analytics sharing, privacy features, and location-sharing settings
- □ Use a vulnerability scanning tool to identify misconfigurations or outdated software
- □ Identify and replace systems nearing end-of-life
- □ Disable remote administration if unnecessary



Physical and Network Security

- □ Physically secure all devices to limit tampering
- □ Connect devices to secure networks with strong encryption
- □ Implement network discovery tools or other processes to detect and/or prevent unknown, unmanaged, or new devices from being plugged in without the IT department knowing
- □ Identify listening devices (e.g., Amazon Echo) that may be located in areas where sensitive information or conversations are being held
- □ Ensure devices are behind a firewall configured with ingress/egress filtering to prevent malicious data from coming in and to prevent the device being used to send data out

Disaster and Incident Response

- □ Incorporate into business continuity, disaster recovery, and incident response plans and consider the impact if devices stop working (e.g., what happens in power-loss scenarios where the alarm system is no longer functioning or cannot connect to the Internet)
- □ Implement redundant Internet connections with automatic failover for critical devices
- □ Configure alerts or other monitoring tools to identify and escalate suspicious activity
- □ Ensure disruptions in power or Internet do not reset the device to an unsecured state

Learn more about how CapinTech can help you assess and reduce your organization's cybersecurity risk at capintech.com