Top 10 Shadow IoT Wireless Risks

LOCH

The availability of IoT devices is causing employees to bring these devices into corporate and operational facilities. The majority of IoT devices are wireless, making them more difficult to detect, creating a blindspot for organizations, an evolution known as Shadow IoT. If left unresolved, Shadow IoT devices and networks can impact Operations, Facilities, Physical Security, Network Security, Data Privacy, and Safety of employees, customers, or patients. The following is a list of common Shadow IoT risks.

Wireless Thermostats

Attackers can connect to open or unconfigured thermostats, adjust the temp and overheat datacenters, hospitals, etc.

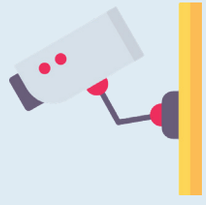
Wireless Thumb Drives

Thumb drives are now wireless. Employees commonly leave these unconfigured, allowing anyone to steal the data

Voice Assistants

Vulnerabilities have been found in these allowing eavesdropping on conversations. Many act as a bridge to the WiFi network.

Surveillance Cameras



Surveillance Cameras are becoming more wireless and now vulnerable to wireless attacks, interception, eavesdropping and disruption

Drones

Drones can be used to disrupt wireless networks, case a facility for break-ins or attacks, or drop a pathogen causing safety risks

Impact

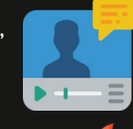
Data Center Disruption

Malware Infestation

Data loss, credential theft, and privacy exposures

Power or Operations Outage

Eavesdropping, IP Theft, Espionage



Safety including fires, pathogens, floods

Smart TVs

Smart TVs are everywhere. If left unprotected, hackers can access the TV to plant malware, steal credentials, or eavesdrop on a board meeting.

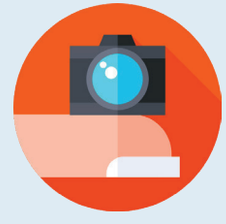
Wireless Printers

Wireless printers are now in every office. When left open, attackers can connect and access print jobs, facsimiles, plant malware, or backdoor the network

Medical Devices

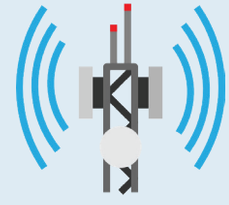
Medical devices are susceptible to a variety of wireless risks including disruption and access to patient data, all causing safety issues for patients

Spy Cameras



That wall charger, clock, or bulb may be a spy camera! These wireless IoT devices allow secret surveillance commonly transmitted to a mobile device.

Rogue Cell Towers



Rogue cell towers have been documented in DC, Las Vegas, and other cities. Recent reports in 2019 revealed 4G and now 5G are also vulnerable to attacks putting devices at risk