Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR
CYBER SECURITY

Internet of Things (IoT) Security

July 2022

ITSAP.00.012

What is the IoT?

The IoT refers to the network of everyday web-enabled objects that can connect and exchange information. These "smart" objects include more than your average computer, smartphone, or tablet. They include items like personal fitness trackers, TVs, thermostats, or connected cars. This list of IoT devices is continuing to grow. IoT Analytics[1] projects that there will be more than 30 billion IoT connections by 2025, with an average of four IoT devices per person. Understanding how to securely use IoT devices in your organization is increasingly important.

How does IoT work?

IoT devices require little to no input from you after their initial set-up is complete. They have embedded sensors, electrical components, and software that collect data and information from their surroundings. The data is sent over the Internet to the cloud for processing, where it is shared with other network-connected devices through Bluetooth, Wi-Fi, or Radio-Frequency Identification (RFID) technologies.

How are IoT devices changing workflow?

IoT devices make routine tasks and processes more efficient and convenient, saving time so that employees can focus on other priorities. For example, you might use a mobile payment device attached to a smartphone for a simple, portable payment method.

By using IoT devices, your organization can save money. For example, the use of automated heating and cooling management systems saves energy and reduces the cost of utilities.

What are some examples of organization-related IoT devices?

When you look around your workplace, IoT devices might not always be obvious at first glance. Examples of IoT devices include:

- Teleconferencing equipment
- Smart boards
- Smart speakers and other voice-activated devices
- Intelligent equipment sensors
- Smart meters (e.g. electrical and water meters)
- Intelligent motion sensors and air sensors
- Networked security cameras
- Corporate vehicle fleets
- Multifunction devices (MFD) (e.g. printers, fax machines)
- Smart appliances (e.g. kettles and fridges)
- Point of sale (POS) systems
- Modern building control systems (e.g. HVAC, electrical, water)
- Corporate mobile phones and portable IT equipment
- Smart watches or fitness trackers

Note: Allowing employees to bring their own smart devices to work can introduce more security risks.

For details on mobile devices in the workplace, see *End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)*.

AWARENESS SERIES

Cat. No. D97-1/00-012-2022E-PDF
ISBN 978-0-660-43938-9

Canada

What are the risks?

Current IoT devices may have inadequate security control and encryption capabilities, leaving devices vulnerable to potential threats. Threat actors can take advantage of device vulnerabilities, such as in the following examples:

- Compromising environmental control systems and smart appliances (e.g. coffee maker, building heating and electrical) in physical workspaces could lead to profit losses (e.g. tampering with temperature controls in a server room, causing equipment malfunction)
- Gaining unauthorized access to company building security controls (e.g. unlocking doors, viewing surveillance cameras)
- Taking control of MFDs to maliciously disrupt Internet access (e.g. Mirai botnet attack)
- Accessing microphones remotely on IoT devices to listen in on sensitive conversations
- Taking control of a car's safety features (e.g. tampering with a vehicle's brakes)
- Controlling a hospital's medical equipment (e.g. interfering with magnetic resonance imaging [MRI] systems)
- Accessing sensitive data or personal information (e.g. customer names and credit cards) through unsecured IoT devices that are connected to company networks

How does IoT impact critical infrastructure?

IoT is often used for industrial operations (e.g. manufacturing, energy, transportation, medical) that contribute to critical infrastructures (CI). IoT offers machine-to-machine communications to enhance business processes by optimizing productivity, safety, sustainability, and cost.

With these enhanced business processes, industrial operations and CI can be at greater risk when using IoT. Having multiple devices connected to systems that handle highly sensitive functions can risk external vulnerabilities affecting processes and provision. Multiple connections to devices, IT networks, and the internet, offer cyber criminals more angles to attack your systems from.

For more details refer to Security considerations for critical infrastructure (ITSAP.10.100), on our website.

How can I keep IoT devices secure?

Before introducing IoT devices into your organization, you should investigate the security capabilities and understand the types of data that the devices send and receive. As more IoT products are brought into the workplace, your organization should implement plans and policies to minimize the possibility of cyber security incidents on your network. Your plans and policies should address the following considerations:

- Restricting personal IoT devices to a separate bring-your-own-device (BYOD) network (e.g. guest Wi-Fi)
- Changing the default passwords on IoT devices. If password rules allow, use passphrases, rather than passwords, on all IoT devices in the workplace
- Using two-factor authentication for devices or apps to add an extra layer of security
- Ensuring data generated by IoT items is encrypted
- Turning off any automatic connection services (e.g. plug and play)
- Updating and patching IoT devices with the most current software (if the product allows)
- Monitoring, detecting, and correcting any IoT security issues (your vendor can assist with this process)
- Isolating IoT networks to restrict access with systems managing sensitive data
- Researching reviews and security ratings on manufacturers and products

What should I remember?

IoT devices can help find efficiencies in workflows and processes, but your organization inherits the security issues of any connected device. If used in the workplace, employees may have privacy concerns if their movements and work activities are monitored by smart technology.

Your organization should implement policies to ensure IoT devices are introduced, used, and managed securely. There should also be policies enforcing appropriate data storage on all devices.

REFERENCE:

[1] IOT ANALYTICS. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time, November 2020.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (CCCS) at cyber.gc.ca