AVOIDING THE PERILS OF A CONNECTED WORLD: NEW BEST PRACTICES FOR RISK MITIGATION

Posted on August 31, 2022

Categories: Insights, Publications

On August 25, 2022, the Canadian Center for Cyber Security ("**CCCS**") released updated guidance on risk mitigation when using internet of things ("**IoT**") devices, which provides new and important considerations for business activity.[1]

What is Internet of Things?

IoT refers to the network of everyday web-enabled objects that can connect and exchange information, and are often referred to as "smart" objects. Items that use the IoT network include not only laptops and smartphones, but also items like personal fitness trackers, TVs, thermostats, connected cars and home surveillance devices. IoT devices use the Internet to send data to the cloud for processing, where it is then shared with other network-connected devices through the use of Bluetooth, Wi-Fi or RFID technology.

Why is this guidance important?

The use of proper security and privacy protection is increasingly important in the context of these devices, with CCCS projecting that by 2025, there will be more than 30 billion IoT connections with an average of four IoT devices per person.

With capabilities to improve workflow and productivity, IoT devices are often used to make routine tasks more efficient and convenient. For example, using a mobile phone payment device attached to a smartphone makes for for a simple, convenient payment method. From an organizational perspective, uses for IoT devices include teleconferencing equipment, voice activated devices, networked security cameras, and corporate mobile phones, among many others.

What are the privacy and security implications of IoT technology?

IoT technology can create incredible upside for companies that wish to leverage the technology to facilitate a more creative, efficient and innovative environment for employees to succeed in their roles, but can also pose a high level of security risk for the business. Organizations that allow employees to bring their own smart devices to work can pose even more risk to security.

Without proper oversight and consideration, IoT devices can leave a business' network and data vulnerable to numerous potential threats. Threat actors can take advantage of these vulnerabilities, causing a compromise of internal systems, including unauthorized security access to items like mobile Internet-enabled microphones without consent to listen in on conversations, or maliciously disrupting Internet access.

In a broader context, the security of IoT devices also applies to critical infrastructure used in industrial operations (i.e. mining, energy, transportation or medical) which can pose a broader risk to the public and business community at large.

How can businesses protect against IoT threats?

Organizations must carefully consider the implications of deploying these devices in connection with their businesses. To keep IoT devices secure, the CCCS recommends implementing or updating an organization's plans and policies that identify the security capabilities and possible vulnerabilities of an organization's network. In particular, the updated guidance recommends:

- the use of two-factor authorization for devices and applications to add additional layers of security;
- disabling automatic connection services;
- the use of passphrases rather than passwords on all workplace IoT devices; and
- ensuring that data generated by IoT items is encrypted.

Additionally, the CCCS recommends that organizations remember that IoT devices can help find efficiencies in workflows and processes, but an organization inherits the security issues of any connected device on the network. If used in the workplace, the organization should implement policies to ensure IoT devices are introduced, used, and managed securely. Finally, there should also be policies enforcing appropriate data storage on all devices.

If you have any questions about these guidelines, maintaining compliant privacy and cybersecurity policies, or about privacy and cybersecurity more generally, a member of our Privacy & Data Protection Group would be happy to assist you.

[1] Canadian Centre for Cyber Security, *Internet of Things: CCCS Best Practices for Risk Mitigation* (August 25, 2022), available here.

by Robert Piasentin, Kristen Shaw and Hailey Lonsdale (Articled Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2022