Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

UNCLASSIFIED

Connected communities

January 2023

ITSAP.00.222

Our lives are increasingly linked to a wide range of information and communication technologies (ICT) that allow us to interact with the digital world. In a connected community, technologies collect and analyze data about the environment, bridging the real world around us with digital systems, to improve the efficiency of public infrastructure and city operations. These spaces are more commonly known as "smart cities" but can also be referred to as connected cities or places that use smart systems.

Large amounts of data are collected through various devices, such as cameras and sensors, that are connected to internet of things (IoT) and industrial IoT (IIoT) networks. Despite their potential to optimize the world we live in, connected communities come with serious security challenges due to widened attack surfaces for threat actors to exploit and cause injury in the real world. The data collected and stored by connected systems is highly sensitive and requires protection.

What does a connected community look like?

Traditional infrastructure is comprised of hardware and software components that are independent of each other. Connected communities are made up of physical infrastructure embedded alongside digital infrastructure such as connected sensors, networks, algorithms, IoT and wireless devices, applications, and others. This integration creates cyber-physical systems, which are an advanced form of operational technology (OT), that have the potential to transform the quality of living for citizens. OT refers to hardware and software used to monitor and cause changes in processes that affect the physical world. A few examples of how public infrastructure and services can look in a connected community include the following:

Transportation: Cameras and other sensors in traffic signals or street lights, as well as in vehicles, cellular devices, and GPS, can collect real-time information about traffic conditions. This data can then be used to suggest alternate routes, ease congestion, and support emergency vehicles.

Waste and pollution: Sensors on collection bins can identify which are full and notify waste management services to empty specific bins, rather than disrupting an entire route. IoT technology is also an important part of recycling waste to produce energy, monitor air quality to assess pollution levels, and improve wastewater management systems.

Energy: Smart meters allow communities to monitor energy use and lower carbon emissions. An advanced metering infrastructure collects data from public utilities including electricity, gas, heat, and water meters to monitor efficiency. Another example is smart lighting that activates only when needed to help reduce wasteful consumption.

Governance: Many countries are in consultation with industry and government bodies to establish legislation and regulatory frameworks to establish standards. The aim of these standards is to enhance cyber safety, normalize product labeling, and promote improved auditing and compliance. This is important where the safety of citizens or impacts to cyber critical systems are concerned.

AWARENESS SERIES

Cat. No. D97-1/00-222-2023E-PDF
ISBN 978-0-660-46911-9

Canada

What are the challenges and risks of connected communities?

The nature of interconnected critical infrastructure, centralized networks, and the immense amounts of data collected through connected communities present significant challenges and security risks to your organization. An attack on a connected community's infrastructure could disrupt critical functions and exploit personal and corporate data. Following are a few examples:

- **Data breaches** have, over time, led to a huge amount of accumulated information available for threat actors to exploit. Data on a government , location data, energy consumption data, or corporate data all provide sensitive details about an individual's daily life platform, personnel information, or business planning documents.
- **Cyber attacks** are widespread in connected communities because they are not contained within one system. An increased attack surface allows threat actors to target one aspect of vital infrastructure, causing **spillover** effects on other systems.
- Integrating unsupported or outdated infrastructure can be challenging for organizations and need to be handled with care if they were not intended to be connected. Vendor agreements may also not support ongoing maintenance of **legacy** systems.
- Developing **legislation** and **legal frameworks** on how data should be collected to protect citizens is challenging. It may also be difficult for individuals to "opt out" of having their personal data collected.

Cyber-physical systems present new types of risks that differ from ICT and OT systems. Mitigation strategies for connected communities will depend on the type of technologies involved, how they are being used, and the specific risks involved.

Although it may not be possible to apply all reasonable mitigations to all types of infrastructure, the following are some mitigations that could be available to your organization.

- Conventional security strategies may be available to protect systems and networks but require careful review by vendors and subject matter experts. These include methods such as network zoning, monitoring, access controls, firewalls, multi-factor authentication, and end-to-end encryption.
- Privacy and security risk assessments are crucial and must be performed before deploying connected applications or platforms. This includes identifying the risks and preparing, practicing critical incident responses, and mandating routine patching of software components.
- Developing policies and procedures to protect data and providing education centered on awareness and transparency through public consultation helps citizens feel confident living in their connected community. For example, transparency on how data is collected, stored, and used allows for informed consent. In addition, implementing privacy measures ensures that only necessary information is collected.

The following publications provide details and guidance on the different systems briefly outlined in this publication:

- Protect your operational technology (ITSAP.00.051)
- Developing your incident response plan (ITSAP.40.003)
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- Wi-Fi security (ITSAP.80.002)
- Baseline security requirements for network security zones (version 2.0) (ITSP.80.022)
- Developing your IT recovery plan (ITSAP.40.004)
- Preventative security tools (ITSAP.00.058)

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 (Cyber Centre) at **cyber.gc.ca**