Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

An Introduction to Securing Smart Places

First published: November 2022

Introduction

Smart places, also known as smart cities, are places designed to provide enhanced services to citizens using a collection of smart information technology (IT)-enabled systems and devices that capture, communicate and analyse data. To achieve this purpose, previously discrete technologies and systems are interconnected to allow for large-scale coordination, real-time decision making, and increased visibility and situational awareness of the smart place's status.

The large-scale deployments of these interconnected systems and devices has the opportunity to improve the lives of citizens, and increase economic productivity with minimal citizen interaction.

This publication uses smart places as a broad overarching term, which would encompass (but are not limited to): cities, suburbs or neighbourhoods; mine sites; oil rigs; ports; manufacturing and refinery facilities. Although the implementation of a smart place can take many forms, it will often include technologies and systems such as the following:

- Internet of Things (IoT) devices
- operational technology
- sensors
- cloud computing services.

Examples of smart places technologies

- **Smart meters**
  - These are technologies that can remotely measure and collect consumer energy data, be controlled remotely, and detect power outages and faults faster than traditional methods.
  - Smart meters and IoT sensors can work together to achieve electricity grid efficiency in a smart place.
- **Traffic light systems**
  - Sensor networks around a road may use technologies such as cameras, radar, Bluetooth and/or Wi-Fi to collect real-time data, such as congestion, speed and weather conditions.
  - Data is then sent to a control system that uses this information accordingly to improve the flow of traffic, give priority to nearby pedestrians and reduce congestion.

Security risks in smart places

The highly-connected nature of a smart place creates efficiencies for users, and provides finer control and oversight of the place's operation to its implementers, but also presents an increased risk profile. The interconnection of systems and devices at scale complicates and amplifies existing security risks in individual technologies, enables pivoting between previously separate infrastructures and results in an overall larger attack surface. The storage of aggregated or sensitive data and potential connection to critical systems, including critical infrastructure, make smart places an even more attractive target for malicious actors.

System failures in smart places could have significant consequences, even without the involvement of malicious actors, due to poor requirements gathering, design, engineering or simple misadventure. For a smart place, this could arise from the connection of legacy equipment, opaque distribution of responsibility and abstract lines of ownership.

Through malicious or non-malicious activity, disruption of a single service may result in cascading effects to other systems, potentially leading to significant consequences for citizens. The impact of failures in a smart place may range from reputational embarrassment and financial loss to a threat to life.

Implementers may secure elements of their individual deployments, however they are unlikely to mitigate the full range of security risks introduced in smart places without using appropriate defence-in-depth and secure-by-design approaches. Below are some of the key security risks that should be considered by implementers.

Internet of Things

IoT devices are often foundational to the increased functionality introduced by a smart place, however these devices are generally built with utility as a priority and security is often absent or an afterthought.

Ensuring the procurement and implementation of IoT devices that abide by the secure-by-design guidance listed below can help form part of building a defence-in-depth approach to securing your smart place.

- *IoT Secure-by-Design Guidance for Manufacturers*.

Supply chain

When technologies that form part of the infrastructure and services of a smart place are procured from third parties, there is potential for supply chain risk, which is further increased when multiple vendors are involved.

Supply chain risk can result in system compromise and disruption due to vulnerabilities introduced during the manufacturing and/or distribution process. It has the potential to have a large scale impact, which is exacerbated by the interconnectedness of smart places technologies. A holistic understanding of these security risks are required to adequately evaluate the implications of adopting smart place technologies.

Smart place technologies must be procured with security in mind and implementers must be satisfied that vendors will implement controls required to satisfy client and stakeholder requirements.

Existing publications and principles to be considered with respect to supply chains include:

- *Cyber Supply Chain Risk Management*
- *Identifying Cyber Supply Chain Risks*.

Operational technology

The most fundamental aspects of what makes a smart place, local government area or city function come from its municipal services and other critical infrastructures, such as water, gas and electricity. The technologies that help control these infrastructures are forms of operational technology (OT).

OT is used in a wide variety of fields to introduce real-world change, and can be as simple as an automated sprinkler system at a park to something as complex as a water or sewerage treatment plant. Understanding what OT your smart place relies on, and appropriately protecting these technologies, is critical for ensuring the ongoing operation of these fundamental services.

As a part of the technological integration found in smart places, IT and OT systems are becoming intertwined to support the rapidly growing demand of citizens, and ensure greater efficiency and cost reduction.

Due to the requirement for OT to have close to zero downtime, these technologies are infrequently upgraded or replaced, and in some cases they are expected to be operational for 20 to 30 years. The difficulty in updating and upgrading these systems can mean that they steadily become more vulnerable over time and unsuited for operation in the current threat environment.

Hybrid approaches for smart places are seeing adoption of Industrial Internet of Things (IIoT) devices, such as smart meters. These are controlled, managed and connected using IT systems to provide flexible capabilities to OT systems never designed for the integration of such functionality.

With this merger of technologies, previously strict boundaries between OT and the outside world are weakened. Existing OT implementations, which did not consider exposure to IT security risks, may be inappropriately exposed to a threat environment for which they were not designed. This can provide malicious actors with increased opportunities to attack these systems, raising the probability of cyber security incidents. Incidents impacting OT have the potential to cause immediate physical effects in a smart place and consequently directly impact those that rely on those services.

Existing publications to be considered with respect to OT include:

- *Protecting Industrial Control Systems*
- *Industrial Control Systems Remote Access Protocol*.

Cloud computing

Cloud computing provides smart places with a mechanism for delivering IT services that scale, through on-demand network access to a shared pool of configurable computing resources. The uses for cloud computing services in a smart place can vary; such as the implementation of corporate management functions on the cloud, data storage and processing through to real-time operations for IoT and sensor networks.

The scope of cloud computing can result in large scale compromise or disruption if the environment is affected by a cyber security incident. An understanding of what type of cloud, ‘as a Service’, or similar externally hosted offerings are used by, connected to or underlie your smart place are imperative to uplifting its cyber security posture.

The procurement, implementation and management of cloud-based services must be appropriately risk managed to ensure the overall security of a smart place. The storage of personally identifiable or other sensitive data on these systems may require further controls be implemented to mitigate the security risks present. In addition, it is important to consider the availability of the cloud service itself, including the availability requirements for the networks used to communicate with the cloud service.

Existing publications to be considered with respect to cloud computing include:

- *Cloud Computing Security for Executives*
- *Cloud Computing Security for Tenants*.

Mitigating security risk

The implementation of smart places technologies can lead to a range of security risks. Understanding and mitigating these security risks is key to securely maximising the potential benefits of these technologies.

Mitigations exist for many of the security concerns currently affecting the technical components of smart places. Exploitation of vulnerabilities can be prevented by implementing secure-by-design principles. To establish an effective foundation for security, implementation of good cyber security practices should be considered. This should be followed by additional environment-specific controls to help achieve a defence-in-depth security posture.

Good cyber security practices for organisations to help better protect their systems and data from cyber threats in a smart places context include:

- *Essential Eight Maturity Model*
- *Strategies to Mitigate Cyber Security Incidents*
- *Information Security Manual*.

In addition, devices connecting, configuring or managing smart place technologies should be hardened to the appropriate standard through existing advice.

Operational redundancy

It is important to consider the interconnectedness and the potential for cascading cyber security incidents in smart places technologies. Implementers must ensure appropriate contingencies for the manual operation for all critical functions, and that staff are trained to enact and action these in case of emergency. These contingencies should plan for the disconnection of smart places technologies from critical services to enable them to operate independently.

In case of a cyber security incident, implementers should have hard copies of both cyber security incident response plans and disaster recovery plans available for all stakeholders. These plans should be easily accessible and practiced by relevant staff, including executive leaders.

Organisations managing a cyber security incident in a smart place should be prepared to isolate systems with as little disruption to critical services as possible.

Implementers must backup relevant systems, ensuring that backups are tested, maintained and properly isolated from outside interference. Backups should be designed to enable offline operation to continually provide the critical service.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate