Management of Industrial Control Systems

Background

The Société de transport de Montréal (STM) provides the population of the Island of Montréal with public transit services, including metro, bus and paratransit.

The metro network consists of 4 lines serving 68 stations over 71 kilometres. This represents a service offer of 85.3 million kilometres travelled annually. The metro is centrally controlled by a Supervisory Control and Data Acquisition (SCADA) System, which monitors and manages the metro's operations. This management requires the use of industrial control systems (ICS) consisting of operational technology (OT) and information technology (IT).

Like all traditional information systems, the ICS can face emerging threats in the form of cyberattacks that cause damage, theft of information, and destruction or alteration of the proper functioning of the metro's ICS.

This report discusses our findings which are public in nature. A separate detailed report has been released internally only due to the highly sensitive and confidential information it contains.

Purpose of the audit

To determine whether the mechanisms in place at the STM ensure the sound management and high degree of availability of the ICS used by the metro.

Results

We conclude that management of the ICS by the STM needs improvements to ensure that it is more effectively managed and to reduce the risks of loss of availability of the metro.

Inadequate management of logical access to the ICS increases the risk of unauthorized access, which could damage the functioning of the metro. In addition, the absence of a formal IT recovery plan carries the risk of loss of availability of the ICS.

Several other elements require improvements, in particular in the areas of:

- → Formalizing roles and responsibilities;
- → The absence of an awareness program specific to the metro's ICS;
- → Systems monitoring; and
- → The comprehensiveness of the change management process.

Nonetheless, the STM has the following adequate control mechanisms:

- → The Division Livraison des services technologiques métro's human resources are adequate;
- → The IT/OT architecture is documented, with adequate segmentation of the networks;
- → The firewalls are regularly updated.

Main Findings

Roles and responsabilities

→ There is no formal document detailing the sharing of roles and responsibilities for the metro's Industrial Control Systems.

Sufficiency and Suitability of Human Resources

→ The human resources in place at the Division Livraison des services technologiques métro are sufficient to meet its needs.

→ There is no awareness program specific to the metro's ICS for the resources of the Division Livraison des services technologiques métro.

Management of Logical Access

→ Logical access control frameworks are not adapted to the metro's ICS, nor systematically applied.

Security of the Industrial Environment Networks

→ The technology architecture is documented and consists of an adequate segmentation of the networks.

→ The firewalls are regularly updated.

→ There is no formal assessment mechanism or procedure for installing updates on the ICS server.

Systems Monitoring

→ A monitoring and security incident warning tool is in place. However, there is no monitoring framework for the metro's ICS.

Change Management

→ A formal change management process is applied. However, it is incomplete according to sound industry practices.

IT Recovery of Systems

→ There is no formal recovery plan for the computer systems.

In addition to these results, we formulated various recommendations to the business units, which are presented on the following pages.