REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System

Date: January 24, 2020
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

This report involves the security of property belonging to the City or one of its agencies and corporations.

The attachment to this report contains information explicitly supplied in confidence to the City of Toronto which, if disclosed, could reasonably be expected to impact the safety and security of the City and its services.

SUMMARY

Some critical infrastructure at the City, such as the Toronto Water treatment plants, use Operational Technology (OT) systems called industrial control systems (ICS). ICS systems include supervisory control and data acquisition (SCADA) systems. SCADA systems monitor and control the equipment and devices used in critical infrastructure.

The Canadian Cyber Security Centre describes how ICS and SCADA systems are vulnerable if appropriate cybersecurity protections are not in place:

> *"As part of the drive for modernization and efficiency, critical infrastructure providers are continuing to automate their processes and connect IT and OT devices to the Internet. While connecting OT, such as ICS and SCADA devices, to the Internet provides several advantages — for example, remote management — it can also expose critical infrastructure to cyber threat activity [1]".*

The objectives of the audit were to assess the adequacy of controls in place to address potential threats to the Toronto Water SCADA network, systems and applications, and to review the actions taken by Toronto Water to address concerns raised during the 2019 cybersecurity audit.

This public report contains two administrative recommendations. The confidential audit findings and recommendations to improve physical security and cybersecurity controls

1 https://cyber.gc.ca/en/guidance/increasing-cyber-threat-exposure

are presented separately to this report in Confidential Attachment 1. Management has already initiated actions to address the identified risks.

The confidential report will be made public at the discretion of the Auditor General after discussing with appropriate City Official.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council adopt the confidential recommendations contained in Confidential Attachment 1 to the report (January 24, 2020) from the Auditor General.

2. City Council direct that all information contained in Confidential Attachment 1 to the report from the Auditor General be *released* publicly at the discretion of the Auditor General after discussing with the appropriate City Official.

FINANCIAL IMPACT

Implementing the recommendations in this report will strengthen both physical security and cybersecurity controls at Toronto Water facilities. We have recommended the City Manager to forward this report, with redaction, as a Confidential Report on an as needed basis to selected Division Heads who are responsible for similar SCADA systems and request that they review and consider implementing the recommendations that are relevant to their respective operations.

The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investments needed to improve controls to manage and respond to cyber threats likely offsets the costs that could result from security breaches, which could include, recovery of infrastructure systems, data recovery/cleanup, financial loss, reputation damage, fines and litigation.

DECISION HISTORY

Considering the importance of cybersecurity of critical infrastructure assets, the Auditor General expanded the penetration testing and vulnerability assessment of the corporate IT network to include Toronto Water SCADA network as a separate project.

COMMENTS

Critical Infrastructure and SCADA Systems

Critical Infrastructure: According to Public Safety Canada:

> "*Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. …Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence* [2]*."*

SCADA Systems: Supervisory Control and Data Acquisition (SCADA) systems are used in a variety of critical applications and industries including energy, utilities, transportation and water. This is a computer system used to monitor and analyze real-time data, and control both local and geographically dispersed industrial processes.

Current risks

The City uses supervisory control and data acquisition (SCADA) system to manage some critical infrastructure water treatment plants, waste water treatment and traffic signalling systems.

The Canadian Centre for Cyber Security describes an increasing cybersecurity threat exposure to critical infrastructure in its publications [3]".

The U.S. Department of Justice in a July 2018 report prepared by the Attorney General's Cyber Digital Task Force describes an attack on a SCADA system:

> "*This is not a hypothetical threat: one of the Iranian hackers indicted for the DDoS attacks against the U.S. financial sector is also alleged repeatedly to have gained access to the Supervisory Control and Data Acquisition ("SCADA") system of a dam in New York, allowing him to obtain information regarding the dam's status and operation. Had the system not been under maintenance at the time, the hacker would have been able to control the dam's sluice gate* [4]*".*

In May 2019 Public Safety Canada's National Cyber Security Strategy also mentioned the importance of cybersecurity:

> "*Criminals and other malicious cyber threat actors — many of which operate outside our borders — take advantage of security gaps, low cyber security awareness, and technological developments in an effort to compromise cyber systems. …They disrupt and sometimes destroy the infrastructure that we rely on for essential services and our way of life* [5]*".*

2 https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx
3 https://cyber.gc.ca/en/guidance/increasing-cyber-threat-exposure
4 https://www.justice.gov/ag/page/file/1076696/download
5 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Toronto Water's SCADA System

Toronto Water Division is responsible for treating, transmitting and storing drinkable water for all industrial, commercial and household water users in the City of Toronto and parts of York Region. It also treats waste water from the City of Toronto and parts of Peel Region. The SCADA system controls highly critical infrastructure equipment and processes that impact Toronto residents, businesses, industries and the environment.

The Audit

The Auditor General tested the cybersecurity of the City of Toronto's SCADA system to ensure the City is protected from cyberattacks and ready to adapt to emerging threats. Opportunities to improve physical security and cybersecurity are reported in the Confidential Attachment 1.

The Auditor General will continue to test more critical systems in separate audits in coordination with management.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We express our appreciation for the co-operation and assistance we received from management and staff of the Toronto Water Division. The timely provision of information and coordination of various activities by the designated team at Toronto Water greatly assisted in completing this audit in a short amount of time. We would also like to acknowledge management and staff from Corporate Security and Office of Emergency Management Divisions.

CONTACT

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, email: syed.ali@toronto.ca

Gawah Mark, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8439, Fax: 416-392-3754, email: gawah.mark@toronto.ca

Suzanna Chan, Audit Manager, Auditor General's Office
Tel: 416-392-8033, Fax: 416-392-3754, email: suzanna.chan@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1 - Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System