TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System - Recommendations Implementation Progress by Management

Date: June 23, 2020
To: City Council
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

The Auditor General completed an audit of the Toronto Water SCADA system in January 2020. The audit focused on the assessment of the adequacy of controls in place to address potential threats to the Toronto Water SCADA network, systems and applications. In addition, the audit also included a review of the actions taken by Toronto Water to address concerns raised during the 2019 cybersecurity audit of the City's IT network.

Toronto Water's SCADA system monitors and controls the equipment and devices used in water infrastructure. The purpose of this report is to update City Council on the progress made by management on the implementation of the audit recommendations made in the SCADA cybersecurity audit.

The Auditor General made 11 confidential recommendations in the SCADA audit. Given the importance of critical infrastructure systems and evolving cyber threats, the Auditor General requested management provide an update on the current status of the recommendations for the June 29, 2020 City Council meeting.

The Auditor General will verify management's assertions through retesting when the recommendations are fully implemented. However, based on management's report on the status of the actions taken to date, as outlined in the Confidential Attachment 1, and

the new oversight by the Chief Information Security Officer (CISO), the Auditor General considers the level of risk identified in our confidential report is now reduced to medium.

Cyber threats continue to evolve around the world. In the past few weeks the Australian Cyber Security Centre (ACSC) has warned that *"malicious cyber adversaries"* were taking advantage of the fact that key staff at critical infrastructure facilities are working from home during the pandemic. Power and water networks as well as transportation and communication grids were threatened[1]. The ACSC has provided guidance to reduce risks of working remotely when operating SCADA networks[2].

Australia's Prime Minister Scott Morrison stated at a news conference last week that our country has been targeted for many months by *"sophisticated, state-based cyberattacks…..This activity is targeting Australian organizations across a range of sectors, including all levels of government, industry, political organizations, education, health, central service providers, and operators of other critical infrastructure*[3].

The Auditor General continues to monitor the progress of implementation of critical audit recommendations. The confidential report tabled at the February 10, 2020 Audit Committee will be made public at the discretion of the Auditor General after discussing with the appropriate City Official.

In addition to follow-up of outstanding recommendations, the Auditor General will continue to audit other critical infrastructure systems and will report to Council on audit findings and management actions to address cyber risks.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council direct the City Manager that all information contained in the Confidential Attachment 1 to the report from the Auditor General to remain confidential.

[1] https://www.cyber.gov.au/news/safeguarding-australias-critical-infrastructure-from-cyber-attack

[2] https://www.cyber.gov.au/advice/covid-19-remote-access-to-operational-technology-environments

[3] https://www.telegraph.co.uk/news/2020/06/19/australia-says-has-target-state-based-cyber-attacks/, https://www.insurancejournal.com/news/international/2020/06/19/572857.htm

FINANCIAL IMPACT

Implementing the recommendations to strengthen both physical security and cybersecurity controls at Toronto Water facilities would assure the supply of safe drinking water to the citizens of Toronto.

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

The Auditor General completed a cybersecurity audit of City's IT infrastructure in October 2019. Considering the importance of cybersecurity of critical infrastructure assets, the Auditor General expanded the audit to include cybersecurity assessment of Toronto Water SCADA network as a separate project.

The Auditor General completed the audit of the Toronto Water SCADA system in January 2020 and the report was tabled at the February 10, 2020 Audit Committee. The public report is available at:

https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

The Auditor General will continue to follow-up implementation of recommendations and will update Council on the actions taken by the management to address potential cyber risks.

COMMENTS

Critical Infrastructure and SCADA Systems

The City uses a supervisory control and data acquisition (SCADA) system to manage drinking water treatment and waste water treatment plants. These are critical infrastructure assets and must be protected.

The Auditor General tested the cybersecurity of the City of Toronto's SCADA system to ensure the City is protected from cyberattacks and preparedness to adapt to emerging threats. The results of the audit were tabled at the February 10, 2020 Audit Committee through a confidential report. This report is being considered at the June 29, 2020 City Council meeting.

The Auditor General requested an interim status update on actions taken by management to address risks identified during the audit. Management advised that the following actions have been taken or are in progress:

- Implementation of multi factor authentication (MFA) at critical entry points
- Improved physical security and monitoring
- Improved IT access controls and monitoring

We express our appreciation for the coordination of management comments by the staff and management of the Toronto Water Division, Technology Services Division, Corporate Services and the Chief Information Security Office.

CONTACT

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

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System - Recommendations Implementation Progress by Management