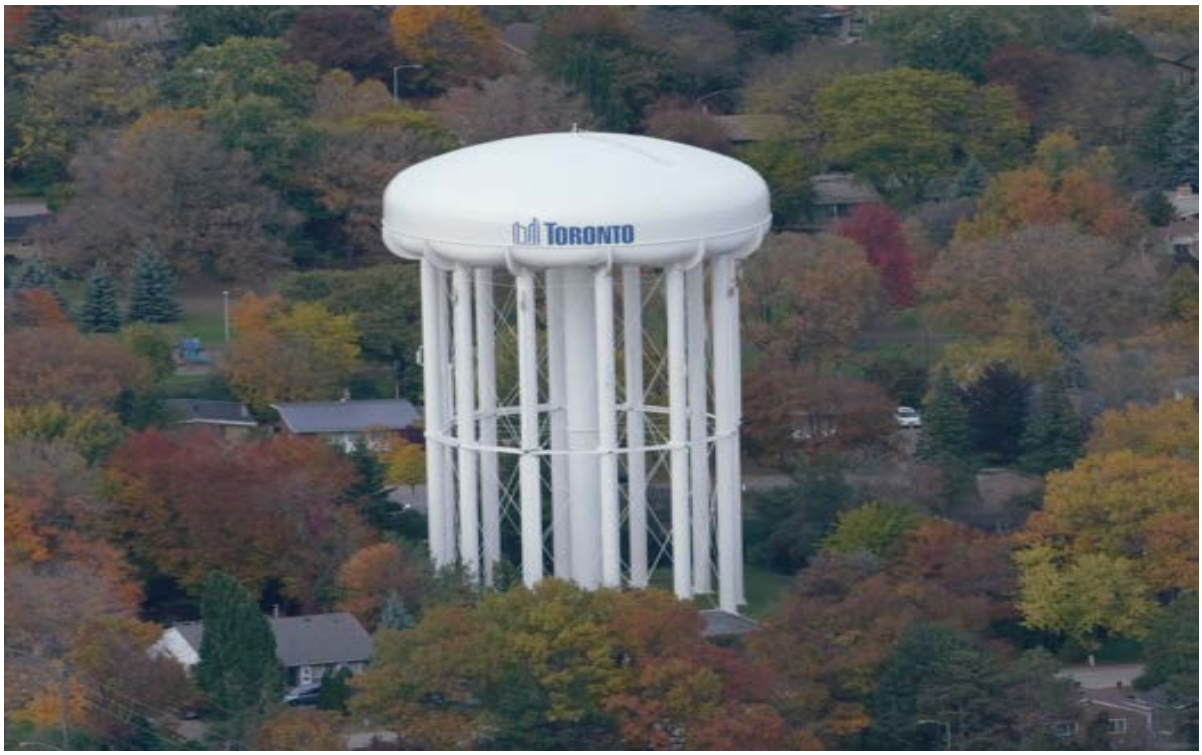
Attachment 1



Toronto Water SCADA System Security

Results of the Follow-up of Previous Audit Recommendations

February 4, 2022

Beverly Romeo-Beehler, FCPA, FCMA, CFF, ICD.D, JD, B.B.A.
Auditor General

AUDITOR GENERAL TORONTO

Table of Contents

Executive Summary

Toronto Water's 2019 SCADA audit was the Auditor General's first cybersecurity audit of critical systems

A SCADA system[1], also known as an Operational Technology (OT) system, is used to control industrial processes at facilities like water and wastewater treatment plants and at energy, utilities and transportation facilities. The 2019 audit of Toronto Water's SCADA system was the Office's first cybersecurity audit of the City's critical infrastructure systems[2].

The Auditor General made 11 recommendations to address various cybersecurity threats. The results were tabled at the February 10, 2020 Audit Committee through a confidential report.

At the November 2021 Audit Committee, we provided a public report and a high-level confidential presentation on the implementation status of our 2019 audit recommendations.

This report includes Confidential Attachment 1, which provides details of management's actions on each recommendation. This report should be considered in conjunction with the Auditor General's Report for Action that was tabled at the November 2, 2021 Audit Committee. The report is available at:

https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172299.pdf

A separate confidential technical report has also been provided to Toronto Water. It should be considered by management in conjunction with this report.

The Auditor General's mandate is to independently verify the implementation status of the audit recommendations management reported as implemented. City Council needs this information to hold management accountable for addressing the risks identified through audits and reviews performed by the Auditor General.

[1] https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition (SCADA)
[2] https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

In preparing audit reports for the Audit Committee and City Council on cybersecurity matters, the interests of accountability and transparency are balanced with the need to manage cybersecurity risks. Many of the original recommendations have been addressed and there has been substantial progress on the remaining recommendations. Therefore, we are able to provide more information in this public report to ensure public transparency and accountability principles are met.

Why the Auditor General conducted an Audit in 2019 and Re-tested in 2021

SCADA system controls Toronto Water's critical infrastructure equipment and processes

A SCADA system controls Toronto Water's water treatment and distribution system. This system is part of the highly critical infrastructure, equipment and processes that impact Toronto residents, businesses, industries and the environment. It is essential that this system is protected from cybersecurity attacks.

In 2019, the Auditor General became aware of attacks on critical water systems in the U.S. and other jurisdictions. In addition, there were a number of alerts issued by the U.S. Department of Homeland Security (DHS), the U.S. Federal Bureau of Investigation (FBI), the Canadian Centre for Cyber Security, and other agencies[3].

The Auditor General was particularly concerned when she learned of a threat published by the U.S. Attorney General, Cyber Digital Task Force describing that:

> *"Iranian hackers… 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]."*

Given that cyber threats continue to evolve, we performed retesting of controls at Toronto Water facilities and SCADA network and systems to verify management actions addressing the 2019 audit findings.

[3] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[4] https://www.justice.gov/archives/ag/page/file/1076696/download

Auditor General's 2021 Follow-up

Vulnerability assessment, penetration testing and onsite physical security assessment was performed

2 facilities added to this follow-up review

We reviewed information provided by management and conducted work to verify the status of recommendations reported as fully implemented. We completed a vulnerability assessment, penetration testing and onsite physical security assessment at selected water facilities. We visited two additional sites in addition to those originally audited in 2019 to determine if controls have been implemented uniformly across other water facilities.

Increase in Attacks on Water Facilities and Critical Infrastructure in many other jurisdictions

Increasing number of attacks on water facilities and other critical infrastructure systems

There has been an increase in the number of attacks on water facilities and other critical infrastructure systems across North America. These attacks are becoming more sophisticated and focused. The Auditor General provided several examples of these attacks in her Report for Action tabled at the November 2, 2021 Audit Committee[5].

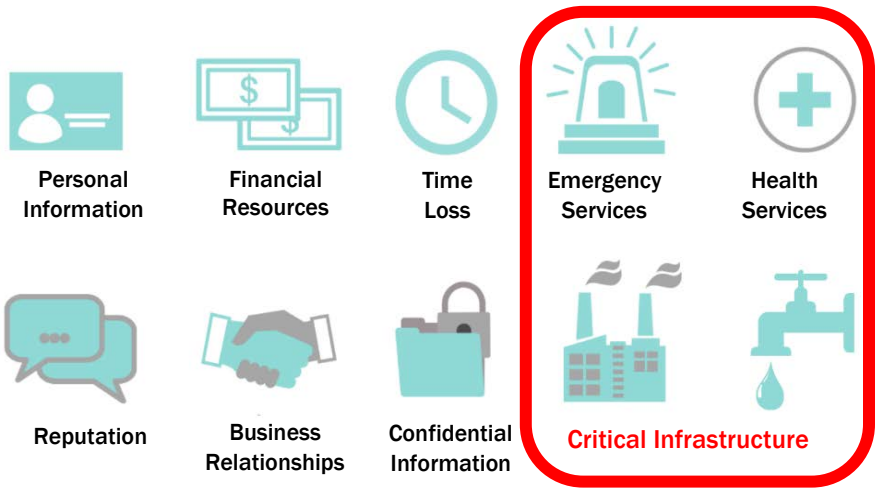
In October 2021, the U.S. Cybersecurity and Infrastructure Agency issued a joint advisory with other security agencies on "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." It stated:

> *"This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities."*[6]:

Figure 1 illustrates targets for cybersecurity attackers, including water treatment and distribution plants that are part of OT.

[5] https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172299.pdf
[6] Ongoing Cyber Threats to U.S. Water and Wastewater Systems | CISA
https://www.reuters.com/article/usa-cyber-water-idUSKBN2H42KY
Ransomware Hit SCADA Systems at 3 Water Facilities in U.S. | SecurityWeek.Com

Figure 1: Critical Infrastructure Is a Target



Auditor General Fast-tracked the Follow-up of Previous SCADA Audit Recommendations

Cyber incidents and high alerts by security agencies indicate serious nature of threats

The incidents in several U.S jurisdictions and official alerts and advisories indicate the serious nature of the threats being faced by water and wastewater facilities, as well as SCADA systems. The Auditor General fast-tracked the follow-up of 2019 SCADA audit recommendations to assess cybersecurity risks and controls implemented by management.

Figure 2 provides a list of attack vectors considered as high risk by the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

In Table 1 of the Confidential Attachment 1, we aligned our 2019 findings to each of the vectors of attack[7] provided below in Figure 2, and our corresponding 2021 results from re-testing. In Table 2 we provided the current implementation status of the 2019 recommendations.

[7] Ongoing Cyber Threats to U.S. Water and Wastewater Systems | CISA

Figure 2: Cybersecurity High-Risk Attack Vectors

Significant work undertaken to follow-up recommendations

To verify the implementation status of the audit recommendations, we undertook significant work to re-test the physical security at selected water facilities. We also re-tested the network security and user access management of the SCADA network, systems and applications to identify any remaining gaps. This work essentially resulted in the team re-performing many of the procedures it had undertaken in 2019.

Testing Results – progress made by Toronto Water

Overall, we found that Toronto Water has implemented many of the 2019 recommendations and has made substantial progress in many areas. The following are some key areas where the Auditor General found improvements:

- physical security of water facilities and IT equipment
- implementation of technical fixes related to cybersecurity
- discontinuation of outdated systems and devices
- segregation/segmentation of the SCADA network
- staff training and awareness

A detailed description of work we performed is provided in Confidential Attachment 1, Tables 1 and 2.

Toronto Water proactively initiated actions as the 2019 audit was in progress

During the 2019 audit, we did note that Toronto Water proactively initiated corrective actions. For example, Toronto Water promptly disconnected the Toronto water SCADA system from the Corporate IT network to strengthen access controls and provide further security.

Significant improvement was observed and majority of the recommendations have been fully implemented

The Auditor General made 11 confidential recommendations in the 2019 audit. In 2021, we confirmed that 7 out of 11 recommendations have been fully implemented, and that substantial work has been undertaken for the remaining recommendations that are not yet fully implemented. In some cases where we deemed that the recommendation has not been fully implemented, it was because the cybersecurity environment is constantly changing. Our follow-up work also identified a few new weaknesses that needed addressing.

The implementation status is included in Confidential Attachment 1, Table 2.

Conclusion

Results of our testing reported in Confidential Attachment 1 to this report

Cybersecurity attackers are constantly trying to find ways to gain unlawful access to confidential data or to disrupt operations for malicious purposes. Cybersecurity threats are ever evolving and becoming more sophisticated.

Toronto Water has made significant progress in implementing the 2019 audit recommendations. However, there is still some work to do as cybersecurity risks continue to evolve and change. Toronto Water will need to be vigilant and continue to proactively monitor for potential security threats and fix known critical vulnerabilities in a timely manner.

In addition, Toronto Water will need to continue to work closely with other City divisions, such as the Office of the Chief Information Security Officer (CISO) and the Technology Services Division, to reduce cybersecurity risks.

The Auditor General will continue to work with City divisions to perform independent cybersecurity assessments and follow up reviews of the City's critical systems.

Testing Results – Contained in Confidential Attachment 1

Results of our testing reported in Confidential Attachment 1 to this report

Toronto Water's work to implement the recommendations is ongoing. Our Office will continue to follow up and report the progress to the Audit Committee. Recognizing the criticality of water systems and efforts by the management, the Auditor General, as part of her audit process, has coordinated with management to provide ongoing progress of the implementation status of cybersecurity recommendations to the Audit Committee and Council[8].

Table 1 in Confidential Attachment 1 provides a comparison of findings we noted in 2019 compared with the threat vectors included in the joint advisory from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other security agencies[9]. The table also provides actions taken by management as noted in 2021 follow-up.

The implementation status for each recommendation is included in Table 2 of the Confidential Attachment 1, and Figures 3 and 4 in the same attachment show the physical security and technical improvements made by Toronto Water since the 2019 audit.

[8] Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System - Recommendations Implementation Progress by Management Date: June 23, 2020 To: City Council
https://www.toronto.ca/legdocs/mmis/2020/cc/bgrd/backgroundfile-148217.pdf

Toronto Water SCADA System Security – Results of 2021 Follow-up of Previous Audit Recommendations Date: October 20, 2021 To: Audit Committee
https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172299.pdf

Auditor General's Status Report on Outstanding Recommendations Date: June 21, 2021 To: Audit Committee
https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-168540.pdf

Auditor General's Follow-up of the Outstanding Recommendations - Status Update Date: February 4, 2021 To: Audit Committee
https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-163332.pdf

[9] Ongoing Cyber Threats to U.S. Water and Wastewater Systems | CISA

Objectives and Scope

Auditor General has proactively raised concerns about evolving cyber threats to the City

Since 2016, the Auditor General has proactively raised concerns about evolving cyber threats to the City as well as its Agencies and Corporations. Cyberattacks are widely considered to be one of the most critical operational risks facing organizations.

The objective of this cybersecurity follow-up review included an assessment of how effective Toronto Water's controls were to prevent and respond to cyber threats. This follow-up review also evaluated the Division's readiness to respond to a cybersecurity attack.

Scope of review

The scope of this follow-up review included detailed testing of controls at water and wastewater facilities. Our work included:

- scanning for and exploiting known vulnerabilities in Toronto Water's internal network, external network and web applications.
- performing physical security reviews of selected water and wastewater plants and pumping stations.
- reviewing actions taken by management on prior audit recommendations to reduce cybersecurity threats.

Note of Thanks

We express our appreciation for the co-operation and assistance received from management and staff at Toronto Water. The timely provision of information and coordination of various activities by the designated team at Toronto Water has greatly helped us to complete this review in a short period of time. We would also like to acknowledge the support we received from management and staff from the Technology Services Division and the Office of the CISO.

AUDITOR GENERAL TORONTO