REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Audit of Toronto Hydro: Overall Network Security and Cybersecurity Assessment of Select Critical Systems

Date: August 2, 2024
To: Toronto Hydro Corporation
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

Confidential Attachment 1 and Confidential Attachment 2 to this report involve the security of the property of the City of Toronto and its agencies and corporations.

SUMMARY

Toronto Hydro Corporation ("Toronto Hydro") is fully owned by the City of Toronto and employs over 1,300 staff. The company delivers electricity to approximately 793,000 customers in Toronto, representing approximately 18% of all electricity consumed in the Province of Ontario.[1] Information technology (IT) plays an important role in all aspects of Toronto Hydro's operations and is part of the larger ecosystem that is responsible for delivering safe and reliable electricity to the residents and businesses in the city.

Critical infrastructure faces evolving cybersecurity threats

The Canadian Centre for Cyber Security in its Cyber threat bulletin: Cyber threat to operational technology, in its assessment states that:

"Operational technology (OT) plays an essential role in the management of Canada's critical infrastructure…"

"OT is extensively used to automate industrial processes in diverse sectors like manufacturing, resource extraction, and essential services such as electricity, natural gas, and water"

and noted that:

1 https://www.torontohydro.com/documents/20143/193303016/2023-annual-information-form, page 15

"The cyber threat landscape experienced by the OT asset operators in Canada is evolving, and cyber threat actors continue to adapt their activities to try to stay ahead of defenders."[2]

Since 2015, the Auditor General has been proactive in her audits of cybersecurity and has completed several vulnerability assessments and penetration testing of critical systems at the City, and its agencies and corporations.

This report includes three administrative recommendations. The confidential findings of the cybersecurity audit of Toronto Hydro and recommendations are included in Confidential Attachment 1 to this report.

In addition, the Auditor General is also making a confidential presentation to Toronto Hydro's Audit Committee at their August 12, 2024 meeting.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Board receive the public report and Confidential Attachments 1 and 2 from the Auditor General.

2. Toronto Hydro ensure that all information contained in Confidential Attachments 1 and 2 to this report remain confidential.

3. Toronto Hydro forward this public report to City Council through the City's Audit Committee for information.

FINANCIAL IMPACT

Implementation of the audit recommendations will further improve Toronto Hydro's cybersecurity posture. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment needed to improve controls to manage and respond to cyber threats offsets the potential costs that could result from security breaches, which could include data recovery/cleanup, financial loss, reputational damage, fines, or litigation.

2 Cyber threat bulletin: Cyber threat to operational technology

DECISION HISTORY

City Council requested the Auditor General in November 2021 to conduct a cybersecurity assessment of Toronto Hydro.[3] The Auditor General started this audit in 2023 and carried it forward to her 2024 Audit Work Plan. The 2024 Audit Work Plan is available at:

Auditor General's Office 2024 Work Plan and Budget Highlights (toronto.ca)

COMMENTS

With cyber threats evolving across the globe, the City of Toronto and its agencies and corporations must ensure their cybersecurity programs are adapting to new challenges and threats. It is important that organizations must therefore continue with their efforts to keep pace with the evolving demands placed upon them by the rapidly shifting digital landscape.

Notable cyberattacks on the energy sector

- Qulliq Energy Corp – in 2023, the Nunavut power provider suffered a cyberattack that severely affected its IT systems.[4] As a result of the attack's severity, the Government of Nunavut transferred Qulliq's IT systems to the government's network permanently.[5]

- Colonial Pipeline – one of the largest U.S. gas pipelines suffered a ransomware attack in 2021, which shut down its billing operations, resulting in disruption to American fuel supplies.[6]

- Ukraine's Power Grid – the European country has experienced outages caused by cyberattacks over the course of its conflict with Russia, starting with an attack in December 2015 that lasted 6 hours and affected 80,000 customers.[7]

As cybersecurity threats expand and evolve, it is important that the Auditor General continues her audits of cybersecurity so that she can make recommendations to improve security controls across the City, and its agencies and corporations.

This audit included Toronto Hydro's network, systems, and applications security. The confidential findings and recommendations are contained in Confidential Attachment 1

3 https://secure.toronto.ca/council/agenda-item.do?item=2021.AU10.3

4 Cyberattack hits Nunavut's Qulliq Energy Corp

5 GN taking over Qulliq Energy Corp.'s IT system in wake of cyberattack

6 Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack | Georgetown Environmental Law Review | Georgetown Law

7 U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage

to this report. The Auditor General will re-test cybersecurity controls after management has implemented the recommendations.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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 Toronto Hydro management and staff.

CONTACT

Syed Ali, Assistant Auditor General, IT and Strategy, Auditor General's Office
Tel: (416) 392-8438, E-mail: Syed.Ali@toronto.ca

Gawah Mark, Audit Director, Auditor General's Office
Tel: (416) 392-8439, E-mail: Gawah.Mark@toronto.ca

Andrew Krupowicz, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-3703, E-mail: Andrew.Krupowicz@toronto.ca

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Toronto Hydro: Overall Network Security and Cybersecurity Assessment of Select Critical Systems

Confidential Attachment 2: Confidential Presentation to the Toronto Hydro Audit Committee of the Board