AUDITOR GENERAL

Halifax Regional Municipality

Halifax Water: SCADA System Audit Public Report

AFSC

March 23, 2023

Audit Scope

- Halifax Water has IT and SCADA systems
- Audit limited to SCADA system
  - Did not include IT systems – except for extent necessary to complete audit

Audit Overview

- Insufficient oversight of SCADA cybersecurity risks
  - Including gaps in policies and procedures
- Physical access controls
  - Management and monitoring of access needs improvement
- Lack of formal policies and procedures to protect SCADA system
  - Such as procedures for changes and updates
- Informal procedures for system availability
  - Lack clear protocols that help limit downtime in emergency
- Also identified improvements in IT

Oversight – Detailed Results

- Lack of corporate oversight of SCADA cybersecurity activities
  - Halifax Water taken steps to address
  - Improvements still needed
- No organization-wide cybersecurity program
  - Cybersecurity strategy does not include SCADA

Oversight – Detailed Results

- Lack of formal project management in Technical Services
  - Developed status updates on outstanding security recommendations for our audit
- Many 2010 SCADA master plan cybersecurity project recommendations not complete

Oversight – Detailed Results

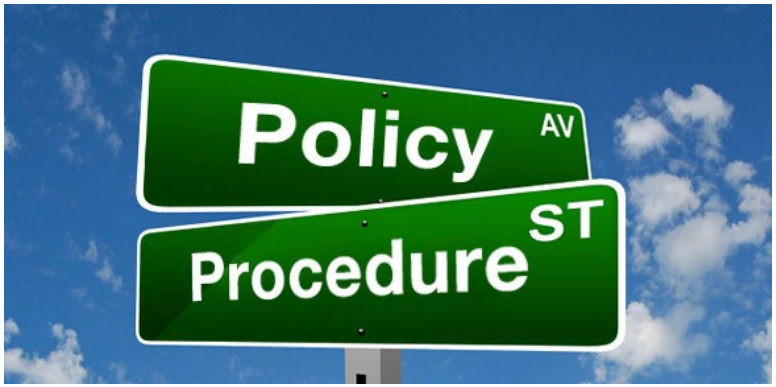
- SCADA security projects and risks not regularly discussed in relevant internal committee meetings
  - Cybersecurity and IT strategic committees
- Not providing Board of Commissioners with regular updates on SCADA security

Oversight – Detailed Results

- SCADA system cybersecurity risks not formally identified and assessed
- Corporate risk register details current and future mitigation strategies
  - Some not in place for SCADA
- No plans or timelines to implement 2016 and 2019 consultant security assessment recommendations

Oversight – Detailed Results

- SCADA cybersecurity policies established and approved 2019
  - Many policies not followed
  - Improvements needed
- Cybersecurity procedures draft since 2016



Physical Access – Detailed Results

- Physical controls at water treatment plants and offices
- No policies or procedures to manage physical access

Physical Access – Detailed Results

- Swipe cards
  - Individuals had access not required for their job
- Keys
  - Manual process to track
  - Tracking spreadsheet not accurate
    - Individuals assigned keys
      - Retired or left Halifax Water
      - Did not require keys for their jobs
    - Instances of keys incorrectly tracked
  - Some keys have not been located

System Protection – Detailed Results

- Lack policies and procedures to protect SCADA system
  - No procedures to manage changes and patches
  - Removable media
  - User-installed software
- No regular SCADA security training and awareness

System Availability – Detailed Results

- Lack clear protocols for some processes which help reduce SCADA downtime in emergency
- No documented policy or procedure for SCADA system backups
- No formal process to document and track spare parts inventory
- Not all critical SCADA assets have been identified
  - Have not determined number of critical assets to keep on hand
  - Spare parts retained in secure areas

Other – IT – Detailed Results

- Halifax Water allowed phishing email to pass through their security settings for our audit
  - Fifty-five Halifax Water employees targeted
    - Forty-five (82%) provided credentials
    - Three (5%) clicked link, but did not submit credentials
- Corporate cybersecurity training offered
  - Further work needed to increase awareness

Other – IT – Detailed Results

- Corporate network has at least 26 user accounts with domain administrator privileges
  - Compromised account could cause widespread damages
- Halifax Water's guest Wi-Fi network not isolated from corporate network

Wrap Up

21 Recommendations

All accepted by management

Halifax Water to implement recommendations

Follow up in 18 months

AUDITOR GENERAL

Halifax Regional Municipality

Questions?