AUDITOR GENERAL

Halifax Regional Municipality

Halifax Water:
SCADA System Audit
Public

March 2023

March 20, 2023

The following audit of **Halifax Water: SCADA System**, completed under section 50(2) of the Halifax Regional Municipality Charter, is hereby submitted to the Audit and Finance Standing Committee of Regional Council.

Respectfully,

Original signed by

Evangeline Colman-Sadd, CPA, CA
Auditor General
Halifax Regional Municipality

AUDITOR GENERAL
Halifax Regional Municipality

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4
www.hrmauditorgeneral.ca
902.490.8407

Table of Contents

Halifax Water SCADA System Audit

Insufficient oversight of SCADA cybersecurity risks

Many 2010 SCADA master plan cybersecurity recommendations not complete

Most 2016 & 2019 consultant recommendations outstanding

Internal committees not regularly discussing risks & plans

Gaps in SCADA cybersecurity policies & procedures

Many policies not followed

Procedures draft since 2016

No policies or procedures for:
- Removable media
- SCADA system backups
- SCADA access

Management of physical access to SCADA needs improvement

Physical access controls at water plants and offices

Informal process to manage swipe card and key access
- Individuals with access who do not require it for their jobs

No monitoring

Informal procedures for system protection & availability

No formal procedures to manage:
- Changes to SCADA information systems
- Patches and updates

No process to manage spare parts inventory
- Have not determined number to keep on hand

Other

Halifax Water IT improvements identified

Sophisticated phishing email targeted 55 employees; 45 (82%) submitted credentials

Auditor General Halifax Regional Municipality

March 2023

Audit Results

Halifax Water manages some risks to its SCADA system. However, there are significant gaps that need to be addressed. The cybersecurity program at Halifax Water is not as mature as we expected for an organization responsible for critical water infrastructure.

There has been insufficient oversight of SCADA security risks. Most consultant recommendations from 2016 and 2019 are still outstanding. Many cybersecurity improvements from the 2010 SCADA master plan are also outstanding. Internal committees are not regularly discussing SCADA risks and plans. In addition, many processes to manage risks to the SCADA system are informal, including cybersecurity policies and procedures and physical access. We also found gaps in processes which could impact the reliability and availability of SCADA operations. This report contains some of our findings in these areas. There is also an in-camera report which expands on the areas reported below and includes a section on network security.

SCADA system cybersecurity risks have not been formally identified and assessed. There have been recent reports of attacks on water SCADA systems in other jurisdictions. The attacks have come from both internal and external threats. As SCADA technology continues to evolve, it is critical that system security risks are effectively managed. If SCADA is compromised it could lead to loss of availability and control of the system, which could impact the water quality and supply.

The scope of this audit was generally limited to the SCADA system which Halifax Water's Technical Services section is responsible for. The audit scope did not include IT systems managed by the Information Services section, except to the extent necessary to complete our audit on the SCADA system.

Oversight

There has not been enough focus on SCADA security risks at Halifax Water. Throughout audit planning and fieldwork, we observed that management of IT and SCADA cybersecurity operate in silos. Information Services (IT) has cybersecurity project management, project plans with timelines, and regularly reports to committees on cybersecurity projects. This was not in place for SCADA.

There have been alerts issued by US government agencies highlighting an increase in cyberattacks on critical water systems. In early 2021, a Florida water plant was hacked, and the hackers attempted to poison the water supply. Later in 2021, US government agencies issued an alert to warn of ransomware incidents targeting water facility SCADA systems. Management and oversight bodies should ensure appropriate processes and controls are in place to monitor and protect the system.

There have been recent, positive changes to the organizational structure of SCADA operations at Halifax Water, but further work is needed. While we recognize there are different priorities for IT and SCADA, it is essential that Halifax Water effectively manages cybersecurity risks in both areas. This will help improve the corporate cybersecurity landscape and help inform corporate programs.

Insufficient oversight of SCADA security risks

There was a lack of corporate oversight of SCADA cybersecurity activities, including a lack of central management. Halifax Water recognized there were gaps in oversight and have taken steps to address this issue. In April 2020, Technical Services (SCADA) was moved to the Engineering and Technology Services department from the Water Services department. This brought the management of IT and SCADA into the same department. In mid-2022, Halifax Water hired a senior manager responsible to oversee SCADA, IT, and GIS. While these are important changes, the bulk of our audit period falls after April 2020; improvements are still needed.

There is no organization-wide cybersecurity program. Halifax Water has a cybersecurity strategy that does not include SCADA (Technical Services). Information Services (IT) is in the second year of its four-year cybersecurity strategy. Recently, Information Services and Technical Services worked together to jointly procure cybersecurity services. Management said the plan is to incorporate SCADA into the strategic projects going forward. It is important to formalize this change, including updating program plans and timelines. This will help ensure a coordinated approach to future cybersecurity improvements.

Recommendation 1

Halifax Water should update its IT cybersecurity strategy, including program plans and timelines, to include SCADA (Technical Services).

Management Response

Management agrees. The formal process of including SCADA in the cyber security practice, including plans and timelines, has been completed as of February 2023.

There is a lack of formal project management in Technical Services. Information Services (IT) has a project management team, which includes a cybersecurity project manager. The Information Services cybersecurity strategic projects have plans, timelines, and status updates. In contrast, Technical Services (SCADA) developed status updates on outstanding security recommendations for our audit. We expected SCADA security improvements to be formally documented, tracked, and communicated to senior management.

Many recommendations from the 2010 SCADA master plan cybersecurity project are not complete. In addition, there are inconsistencies on the status of the plan's completion. Senior management told us they finished the work in 2016. Technical Services management told us they are nearing the end of the plan, and most projects are complete. However, they could not provide project status documentation. In addition, implementation of the master plan is listed as a Technical Services responsibility in the 2022-23 annual business plan. Lack of oversight and project management may have contributed to these inconsistencies.

SCADA Master Plan (2010)

• • •

External consultant developed a strategic plan to standardize the SCADA system. There were 14 short-term projects and 5 long-term projects.

In addition, a cybersecurity assessment was completed. The recommendations to improve security were included in a short-term project.

We reviewed the 13 recommendations from the SCADA master plan cybersecurity project and found:

- Eight are still in-progress
- Four are complete
- One was no longer applicable

Although these recommendations were 12 years old when we completed our audit, Technical Services did not have formal plans and timelines for completion.

Recommendation 2

Halifax Water should implement appropriate project management processes for SCADA.

Management Response

Management agrees. Project Management provided by the I&T Project Management Office has been formally commenced within the SCADA program as of February 2023.

Recommendation 3

Halifax Water should develop plans, with timelines, to complete the remaining SCADA master plan cybersecurity recommendations.

Management Response

Management agrees. Plans, timelines, and documentation will be completed.

SCADA security projects and risks are not regularly discussed in applicable internal committee meetings. There is a cybersecurity committee, and an IT strategic committee, which include senior management from both Information Services (IT) and Technical Services (SCADA). The cybersecurity committee meets quarterly, and the IT strategic committee meets every six weeks. We reviewed committee meeting minutes from January 2020 to December 2022 and found there were limited discussions related to SCADA strategic plans and security. While we found Technical Services provided some operational updates, we expected to see regular updates on security risks, projects, and initiatives. It is important senior management obtain relevant and meaningful information to help assess if risks are addressed and projects are completed in a timely manner.

Recommendation 4

Halifax Water should require regular updates on SCADA security risks, plans and projects in management committee meetings.

Management Response

Management agrees. Halifax Water has formalized reporting on SCADA security risks, plans and projects in its cyber security management committee and in enterprise risk management reporting to the Halifax Water Board.

Additionally, Halifax Water is not providing regular updates on SCADA security to its Board of Commissioners. The Board has quarterly cybersecurity updates through a subcommittee. We reviewed the subcommittee meeting minutes from the committee's inception in June 2021 to January 2023 and found there were regular cybersecurity updates (verbal or presentation). The meeting minutes did not indicate if verbal updates included SCADA. For the meetings with a presentation, we found there were no updates on SCADA security projects and risks. In addition, the Board receives an annual cybersecurity update. The 2020 and 2021 updates did not include SCADA cybersecurity. The Board of Commissioners has a responsibility to hold management accountable to implement strategic plans and exercise risk management. Without regular updates, the Board does not have the information it needs for appropriate oversight of cybersecurity at Halifax Water.

Recommendation 5

Halifax Water should provide regular SCADA cybersecurity updates to the Halifax Water Board of Commissioners.

Management Response

Management agrees. Risks and updates will also be addressed at the Cyber Committee and ERM Board committee which meet quarterly beginning March 2023.

Risks to SCADA system security not appropriately managed

Control Area	Current State – Halifax Water	Why It Matters/ Risk

SCADA security risk identification	• Corporate risk register identifies cybersecurity as a top risk
	• Technical Services has not formally identified and assessed SCADA system cybersecurity risks.
	• Technical Services 2019 risk management policy states a security assessment for critical systems must be completed and documented.
	  • This is outstanding
		• Existing SCADA risks have not been formally identified and assessed to determine if action is needed.
		• Executive Management may not be informed of SCADA risks.
		  • This could affect risk mitigation activities and projects getting approved in a timely manner.
		  • Persistent gaps could allow hackers to penetrate Halifax Water's SCADA system.

SCADA security risk mitigation	• No detailed plans to mitigate SCADA risks.
	• Technical Services has not identified and documented the key controls to mitigate risks.
	• The corporate risk register details current and future mitigation strategies. However, some of the cybersecurity mitigation strategies listed are not in place for SCADA including:
	  • Cybersecurity roadmap and strategy
	  • Only includes Information Services
	  • Cybersecurity policies
	  • Gaps identified, many not implemented
		• Risks that are not appropriately addressed could increase the impact and likelihood of an event impacting water operations.

External SCADA security assessments	• No plans or timelines to implement recommendations from 2016 and 2019 consultant security assessments	• Informs the Board and management of control

Control Area	Current State – Halifax Water	Why It Matters/ Risk
	• Nine of ten outstanding • One complete • No discussions in committee meetings relating to progress and implementation of recommendations	weaknesses and helps prioritize where to address security risks. • Security improvements strengthen the organization's security profile and help reduce the likelihood and impact of breaches and attacks.

Recommendation 6

Halifax Water should identify, document, and assess risks to the SCADA system, including developing risk mitigation strategies. This information should be used to determine where to prioritize future cybersecurity assessments.

Management Response

Management agrees. SCADA Cyber Risk Assessment will be created and maintained.

Recommendation 7

Halifax Water should establish documented plans and timelines to complete the outstanding recommendations from the 2016 and 2019 consultant reports.

Management Response

Management agrees. For each recommendation in the 2016 and 2019 consultant reports, Halifax Water will document our acceptance or rejection of the recommendation. Recommendations that are accepted will be scheduled for completion. In addition, another SCADA Cyber Risk Assessment will be performed in 2023.

Gaps in SCADA cybersecurity policies; procedures in draft since 2016

Control Area	Current State – Halifax Water	Why It Matters/ Risk

SCADA cybersecurity policies	• SCADA cybersecurity policies established and approved in 2019
	  • However, we found many policies are not followed.
	• Policies address some cybersecurity key risk areas including risk management, awareness and training and configuration and change management.
	• No policies for access management, system protection and media protection
	• Management of policies needs improvement
	  • No process to review and update periodically
	  • Not monitoring policy compliance
	  • Not formally communicated to staff
		• If policies are not well communicated, processes may be inconsistent amongst staff.
		• Risks may not be appropriately managed.
		• If policies are not regularly updated, they may no longer address existing security risks.

SCADA cybersecurity procedures	• Purpose of procedures is to implement policies
	• Cybersecurity procedures draft since 2016
	• No detailed plans with timelines for when they will be complete
	• Consistent with audit findings that many cybersecurity policies are not followed
		• No formal processes to implement cybersecurity policies, putting the system at increased risk of malicious activity and breaches.
		• Significant gaps in ensuring controls are implemented:
		  • Process owners are not defined
		  • Responsibilities are not clear

Recommendation 8

Halifax Water should review and update its SCADA cybersecurity policies, ensuring they cover all key cybersecurity areas, and formally communicate policies to employees.

Management Response

Management agrees. SCADA Cyber Documentation will be incorporated into the Cyber Program, completed, and communicated.

Recommendation 9

Halifax Water should document and implement its SCADA cybersecurity procedures. This should include developing plans and timelines for when they will be complete.

Management Response

Management agrees. SCADA Cyber Documentation will be incorporated into the Cyber Program, completed, and communicated.

Physical Access

Halifax Water has physical security controls for access to SCADA. However, management and monitoring of access to the SCADA system and equipment needs improvement. Policies and processes to manage swipe card and key access are informal. There are individuals with physical access to SCADA who do not require it for their jobs. It is important this access is restricted and monitored; an attack on the SCADA system and water treatment process could impact the safety of HRM's drinking water.

Physical controls to secure SCADA

Control Area	Current State – Halifax Water	Why It Matters/ Risk
Physical access controls	• There are physical controls at the water treatment plants and offices to restrict access to the SCADA system.	• Restricts who can access critical water infrastructure • Protects SCADA equipment from unauthorized access and physical damage and destruction
Visitor access records	• Visitor logs are maintained at the large water treatment plants and Halifax Water offices.	• Maintains a physical record of who had access to the facility • Allows supervisors to monitor visitor access to sensitive areas
Power equipment and cabling	• SCADA equipment cables were secured at the three water treatment plants we visited. • All cables leaving the equipment areas were covered and protected.	• Protects the SCADA system from accidental or intentional damage
Emergency power	• SCADA locations have emergency power through uninterruptible power supply and generators.	• Allows for continued operations of the SCADA system during a power failure.

Management of physical access to SCADA needs improvement

Control Area	Current State – Halifax Water	Why It Matters/ Risk
Physical access control policy	• No policies or procedures for managing physical access (swipe cards, keys) to offices and operational facilities • No monitoring to confirm physical access is limited	• Employees could be given access to critical infrastructure and systems that they do not require as part of their job duties. • Could lead to unauthorized access to control the water supply.
Third-party access procedure	• No procedure to manage third-party physical access to the SCADA system • Lack details on authorizations required and security precautions taken for external vendors working around SCADA equipment. • SCADA equipment located in secure areas; IT and physical security (external vendor) equipment maintained in the same areas.	• Vendors may pose a security threat to the organization. • Access should be managed to reduce the risk of introducing a threat or vulnerability to the system.

Physical access – swipe card	• Physical access to SCADA needs to be restricted to only those who require it for their jobs.
	• At three water plants and the SCADA office, we found individuals had access they did not require for their jobs.
	  • JD Kline – 14
	  • Lake Major – 15
	  • Collins Park – 11
	  • SCADA office – 32
		• Could allow unauthorized access by someone with ill intent.
		• Physical attacks to the SCADA system could lead to outages and damages.
		• Insider attacks are a significant threat. Limiting who has access to critical water infrastructure is important.

Control Area	Current State – Halifax Water	Why It Matters/ Risk

Physical access – keys	• Manual process to track water plant and distribution system keys
	• Reviewed assigned keys for three water plants, and distribution system buildings.
	• The spreadsheet to track keys was not accurate.
	  • Individuals assigned keys who had either retired or left Halifax Water.
	  • Multiple keys assigned to supervisors to manage; no process to centrally track these keys.
	  • Instances of keys incorrectly tracked as assigned or unassigned, or assigned to the wrong individual.
	  • While some keys have been found, management is looking into the location for the remainder.
	• For the remaining assigned keys, we found individuals who do not require them for their job.
	  • Eleven assigned keys to the distribution system buildings.
	  • Two assigned keys to an individual water plant.
	  • One individual assigned a master key to the plants.
	  • Individual changed positions at Halifax Water and access was not updated.
		• Poor key management may give unauthorized individuals access to critical infrastructure which could lead to tampering and damaging with water and monitoring equipment.
		• Key access does not leave an audit trail the way swipe cards do. It is important keys are accurately tracked and secured.

Recommendation 10

Halifax Water should develop policies and procedures to manage physical access, including regular monitoring.

Management Response

Management agrees. Physical access policies and procedures will be enhanced around the tracking of access with regular monitoring to confirm they are operating as intended.

Recommendation 11

Halifax Water should review existing physical access and remove access that is not required for an individual's job.

Management Response

Physical access policies and procedures will be enhanced around existing access and removal of access will be actioned promptly. The policies and procedures will be monitored regularly to ensure they are operating as intended.

Recommendation 12

Halifax Water should develop a procedure to manage third-party access to the SCADA system which addresses cybersecurity best practices.

Management Response

Management agrees. Halifax Water is in the process of hiring a Cyber Security specialist for the Technical Services Team. This new person will create a policy and procedure for third party access. The policy and procedure will be monitored regularly to ensure they are operating as intended.

System Protection

Halifax Water lacks formal policies and procedures to protect the SCADA system. There are no procedures to manage changes and updates to the SCADA system. There are no policies for acceptable use of removable media or user-installed software. It is important organizations have implemented documented systems with monitoring to prevent unauthorized changes to the system. In addition, Technical Services does not provide SCADA users regular cybersecurity awareness and training on relevant system risks, programs and policies. There are different risks associated with operating SCADA; all users should be informed of their role in helping protect the system.

No documented procedures for system changes and updates

Control Area	Current State – Halifax Water	Why It Matters/ Risk

System changes and updates operating procedures	• No documented procedures to manage changes and patches to the SCADA system.	• Without documented procedures:
		  • Inconsistent approaches to system changes across staff
		  • Nothing to guide new staff
		  • Important updates might be missed.

Recommendation #9 addresses documenting and implementing cybersecurity procedures.

Lack policies to restrict software and removable media

Control Area	Current State – Halifax Water	Why It Matters/ Risk
Removable media acceptable use policy	• No policy for managing the acceptable use of removable media on SCADA computers.	• Limits and controls what can be connected to the SCADA system. • Reduces the risk of vulnerabilities being introduced to the system.

Control Area	Current State – Halifax Water	Why It Matters/ Risk
User-installed software policy	• No policy or procedure to approve and monitor user-installed software on SCADA assets. • Management has a documented list of approved software for SCADA technician laptops. • We sampled three technician laptops and found the software installed mostly aligned with the approved list. • The software not on the list was reasonable for job duties. However, there were no management approvals.	• If employees download personal or unauthorized content, it could contain viruses and malware that could affect the SCADA system. • Due to the critical nature of the SCADA system, only approved and tested software should be allowed on SCADA assets.

Recommendation 13

Halifax Water should develop and implement a policy for acceptable use of removable media on SCADA assets. This should be communicated to all employees who work with or around SCADA.

Management Response

Management agrees. A policy will be created, implemented, and communicated around the use of removeable media at Halifax Water.

Recommendation 14

Halifax Water should implement a process to review, approve, and monitor software installed on SCADA laptops.

Management Response

Management agrees. A process to review, approve and monitor software will be completed.

No regular SCADA security training and awareness

Control Area	Current State – Halifax Water	Why It Matters/ Risk
SCADA security awareness training	• Technical Services does not provide regular SCADA-specific cybersecurity awareness and training on system risks, programs and policies to its staff or users of the SCADA system.	• Important for employees to be aware of their role in protecting SCADA from security risks. • SCADA systems have different risks than typical IT systems which users should be aware of.

Recommendation 15

Halifax Water should provide SCADA system users with regular training or information to increase awareness of SCADA security risks, policies, and procedures.

Management Response

Management agrees. This training is currently part of the Cyber Awareness Training Program and will be provided to technical services staff which will include information on operation and security of the SCADA system.

System Availability

Water treatment processes can be operated and monitored manually but modern technology allows for a more efficient and effective process, using a SCADA system. Halifax Water needs to improve its processes which help maintain SCADA system availability. If current management leaves, there is lack of clear protocols for some processes that help reduce SCADA downtime in an emergency. There is no formal process to backup the SCADA system. In addition, not all critical SCADA assets have been identified. Management told us they use their experience to determine what assets to keep on hand. While we found there are some spare parts on hand, there is no process to document and manage inventory, including ensuring an appropriate number of critical assets are on hand.

We were not made aware of any major failures to the SCADA system during the audit. However, it is important Halifax Water is prepared to handle failures and security events with little or no interruption of water operations or loss of data.

Poor processes to ensure system availability

Control Area	Current State – Halifax Water	Why It Matters/ Risk
SCADA system backup procedure	• No documented policy or procedure for SCADA system backups	• Backups allow for timely recovery of the SCADA system and reduce the loss of data. • Without a documented policy, process to collect backups could be inconsistent and get missed.
Asset management	• Asset management policy outlines inventorying and maintaining physical assets. • No formal process to document and track spare parts inventory • Have not determined the number of critical assets to keep on hand • Positive finding – spare parts are retained in secure areas.	• Adequate number of critical parts are on-hand, helps reduce SCADA downtime during an event or emergency.

Control Area	Current State – Halifax Water	Why It Matters/ Risk

Critical SCADA asset identification	• Not all critical SCADA assets have been identified.
	  • Computers, software and network devices documented
	  • SCADA equipment (PLCs, RTUs) not documented
	• Critical SCADA assets not documented in contingency plans
	  • Helps determine what other resources can be used in an emergency to reduce impact on operations.
		• Important aspect of business continuity and risk management.
		• Identification and location of critical assets should be documented and linked to contingency plans.

Recommendation 16

Halifax Water should implement a process to maintain regular backups of the SCADA system.

Management Response

Management agrees. A process will be created to maintain regular backups of the SCADA system. This process will be monitored and tested to ensure it is operating as intended.

Recommendation 17

Halifax Water should identify and document all critical SCADA assets, including determining the number of spare parts to keep on hand. This should be linked to contingency plans.

Management Response

Management agrees. All critical SCADA assets will be documented to determine the number of spare parts to keep on hand. This will be part of the business continuity plan.

Recommendation 18

Halifax Water should develop and implement a process to track and manage inventory of spare parts.

Management Response

Management agrees. A process will be created to track and manage an inventory of spare parts.

Other - IT

Halifax Water's corporate network could be an entry point for threats looking to access the SCADA network. Our audit scope did not include IT. However, our testing included some aspects of the corporate network to assess potential risks to SCADA. During our testing, we sent a sophisticated phishing email to Halifax Water employees. Test results showed further security awareness training is needed.

Sophisticated phishing email targeted employees; 82% of recipients submitted credentials

Control Area	Current State – Halifax Water	Why It Matters/ Risk

Corporate cybersecurity awareness	• Halifax Water allowed a phishing email to pass through their security settings for our audit.
	  • The purpose was not to test the security controls to prevent a phishing email, but to test staff awareness.
	• Sophisticated phishing email sent; obtained credentials from management and employees across various departments.
	• Fifty-five Halifax Water employees were targeted
	  • Forty-five (82%) employees provided their credentials.
	  • Three (5%) employees clicked the link but did not submit their credentials.
		• Hackers target employees to manipulate them into performing actions or providing confidential information to try and gain access to the network.
		• Employees play an important role in detecting and preventing cybersecurity threats.

Corporate cybersecurity training	• Corporate cybersecurity training offered to employees.
	• Regular cybersecurity training courses were sent to employees from 2018 to early-2022. Management provided us reports on course participation rates. The participation rates varied; we could not confirm this as management no longer had access to the original training records.
	• Mandatory cybersecurity fundamentals course rolled out February 2022. We sampled 30 employees and found six have not yet taken the course as of November 2022.
	• In mid-2022, plans and timelines were developed to roll-out a new cybersecurity training campaign.
		• Increases cybersecurity awareness
		• Employees help overall security when aware of:
		  • Creating strong passwords
		  • Identifying malicious links
		  • Not leaking sensitive information

Recommendation 19

Halifax Water should finalize and implement cybersecurity training awareness campaigns.

Management Response

Management agrees. A cybersecurity awareness training program which includes onboarding training and annual refresher training has been implemented.

Recommendation 20

Halifax Water should follow up to help ensure employees complete mandatory security awareness training.

Management Response

Management agrees. A process has been put in place to ensure all staff compete the mandatory cyber security awareness training.

Corporate network improvements identified

Control Area	Current State – Halifax Water	Why It Matters/ Risk

Domain administrator privileges*
 	
**The highest level of privilege; a user with this access can make changes to all computers and users connected to the organization's active directory database.*
	• The corporate network has at least 26 user accounts with domain administrator privileges.
	  • This privilege allows full control of the network and its resources.
	  • A compromised account could cause widespread damages such as changing domain and user accounts, resetting passwords and installing malware.
		• Poor access management (many domain accounts) makes it easier for hackers to attack the network.

Wi-Fi segmentation	• Halifax Water's guest Wi-Fi network was not isolated from the corporate network. • Segmentation controls were implemented, but not operating as intended.	• Threats can compromise the network without physically entering the building.

Control Area	Current State – Halifax Water	Why It Matters/ Risk
	• Additionally, the password was posted on walls in the head office, visible to the public. • Management said this has been corrected.	

Recommendation 21

Halifax Water should reduce the number of users with domain administrator privileges to a small number who require this level of access for their jobs.

Management Response

Management agrees. This has been completed.

Background

Halifax Water is a municipal utility responsible for providing water, wastewater, and stormwater services to the residents of HRM. The Halifax Water Board of Commissioners provides civilian oversight for Halifax Water.

Halifax Water has a supervisory control and data acquisition (SCADA) system to remotely access and monitor the operations of its water and wastewater plants and distribution systems. Halifax Water's SCADA system is a type of industrial control system that consists of instrumentation, communication equipment, and computer hardware and software. Plant operators use the SCADA system to operate, monitor and make modifications during the water treatment and delivery process.

Technical Services, a section within Halifax Water's Engineering and Technology Services department, is responsible for the operation and maintenance of Halifax Water's SCADA system. This includes SCADA security, electrical work, and maintenance.

Information Services, also a section within Halifax Water's Engineering and Technology Services department, is responsible for corporate IT services including network resources, network security, server hardware and operating systems, computer equipment, corporate software, and cybersecurity.

About the Audit

We completed a performance audit of Halifax Water's SCADA system. The scope did not include Halifax Water's IT system, except for the extent necessary to complete our audit on the SCADA system.

The purpose of the audit was to determine whether Halifax Water appropriately manages risks to its SCADA system. Our role is to express an independent audit opinion of this area.

The objective of this audit was to determine whether Halifax Water manages risks to its supervisory control and data acquisition (SCADA) system to ensure it is secure, reliable, and operationally available.

We developed criteria for this audit. These were discussed with and accepted as appropriate by management of Halifax Water.

- Halifax Water should have processes to ensure risks to the SCADA system are appropriately identified, addressed, and managed.
- Halifax Water should have processes to ensure the SCADA system is reliable and operationally available.

We used NIST Special Publication (SP) 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security and 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations to assess and conclude on our criteria. We did not complete a compliance audit against these frameworks.

Our audit period was January 1, 2020 – November 30, 2022. Information from outside the audit period was considered as necessary.

Our audit approach included: interviews with management and staff; review of internal policies and procedures; testing of key processes and controls; observation of activities, facilities and operations; examination of documents; and a penetration test of Halifax Water's supervisory control and data acquisition (SCADA) system.

The audit was conducted in accordance with the Canadian Standards on Assurance and Engagements (CSAE) 3001 Direct Engagements published by the Chartered Professional Accountants of Canada.

We apply CPA Canada's Canadian Standard on Quality Management 1. Our Staff comply with the independence and ethical requirements of the Chartered Professional Accountants of Nova Scotia Code of Conduct.

Appendix 1 – Recommendations and Management Responses

Recommendation 1

Halifax Water should update its IT cybersecurity strategy, including program plans and timelines, to include SCADA (Technical Services).

Management Response

Management agrees. The formal process of including SCADA in the cyber security practice, including plans and timelines, has been completed as of February 2023.

Recommendation 2

Halifax Water should implement appropriate project management processes for SCADA.

Management Response

Management agrees. Project Management provided by the I&T Project Management Office has been formally commenced within the SCADA program as of February 2023.

Recommendation 3

Halifax Water should develop plans, with timelines, to complete the remaining SCADA master plan cybersecurity recommendations.

Management Response

Management agrees. Plans, timelines, and documentation will be completed.

Recommendation 4

Halifax Water should require regular updates on SCADA security risks, plans and projects in management committee meetings.

Management Response

Management agrees. Halifax Water has formalized reporting on SCADA security risks, plans and projects in its cyber security management committee and in enterprise risk management reporting to the Halifax Water Board.

Recommendation 5

Halifax Water should provide regular SCADA cybersecurity updates to the Halifax Water Board of Commissioners.

Management Response

Management agrees. Risks and updates will also be addressed at the Cyber Committee and ERM Board committee which meet quarterly beginning March 2023.

Recommendation 6

Halifax Water should identify, document, and assess risks to the SCADA system, including developing risk mitigation strategies. This information should be used to determine where to prioritize future cybersecurity assessments.

Management Response

Management agrees. SCADA Cyber Risk Assessment will be created and maintained.

Recommendation 7

Halifax Water should establish documented plans and timelines to complete the outstanding recommendations from the 2016 and 2019 consultant reports.

Management Response

Management agrees. For each recommendation in the 2016 and 2019 consultant reports, Halifax Water will document our acceptance or rejection of the recommendation. Recommendations that are accepted will be scheduled for completion. In addition, another SCADA Cyber Risk Assessment will be performed in 2023.

Recommendation 8

Halifax Water should review and update its SCADA cybersecurity policies, ensuring they cover all key cybersecurity areas, and formally communicate policies to employees.

Management Response

Management agrees. SCADA Cyber Documentation will be incorporated into the Cyber Program, completed, and communicated.

Recommendation 9

Halifax Water should document and implement its SCADA cybersecurity procedures. This should include developing plans and timelines for when they will be complete.

Management Response

Management agrees. SCADA Cyber Documentation will be incorporated into the Cyber Program, completed, and communicated.

Recommendation 10

Halifax Water should develop policies and procedures to manage physical access, including regular monitoring.

Management Response

Management agrees. Physical access policies and procedures will be enhanced around the tracking of access with regular monitoring to confirm they are operating as intended.

Recommendation 11

Halifax Water should review existing physical access and remove access that is not required for an individual's job.

Management Response

Physical access policies and procedures will be enhanced around existing access and removal of access will be actioned promptly. The policies and procedures will be monitored regularly to ensure they are operating as intended.

Recommendation 12

Halifax Water should develop a procedure to manage third-party access to the SCADA system which addresses cybersecurity best practices.

Management Response

Management agrees. Halifax Water is in the process of hiring a Cyber Security specialist for the Technical Services Team. This new person will create a policy and procedure for third party access. The policy and procedure will be monitored regularly to ensure they are operating as intended.

Recommendation 13

Halifax Water should develop and implement a policy for acceptable use of removable media on SCADA assets. This should be communicated to all employees who work with or around SCADA.

Management Response

Management agrees. A policy will be created, implemented, and communicated around the use of removeable media at Halifax Water.

Recommendation 14

Halifax Water should implement a process to review, approve, and monitor software installed on SCADA laptops.

Management Response

Management agrees. A process to review, approve and monitor software will be completed.

Recommendation 15

Halifax Water should provide SCADA system users with regular training or information to increase awareness of SCADA security risks, policies, and procedures.

Management Response

Management agrees. This training is currently part of the Cyber Awareness Training Program and will be provided to technical services staff which will include information on operation and security of the SCADA system.

Recommendation 16

Halifax Water should implement a process to maintain regular backups of the SCADA system.

Management Response

Management agrees. A process will be created to maintain regular backups of the SCADA system. This process will be monitored and tested to ensure it is operating as intended.

Recommendation 17

Halifax Water should identify and document all critical SCADA assets, including determining the number of spare parts to keep on hand. This should be linked to contingency plans.

Management Response

Management agrees. All critical SCADA assets will be documented to determine the number of spare parts to keep on hand. This will be part of the business continuity plan.

Recommendation 18

Halifax Water should develop and implement a process to track and manage inventory of spare parts.

Management Response

Management agrees. A process will be created to track and manage an inventory of spare parts.

Recommendation 19

Halifax Water should finalize and implement cybersecurity training awareness campaigns.

Management Response

Management agrees. A cybersecurity awareness training program which includes onboarding training and annual refresher training has been implemented.

Recommendation 20

Halifax Water should follow up to help ensure employees complete mandatory security awareness training.

Management Response

Management agrees. A process has been put in place to ensure all staff compete the mandatory cyber security awareness training.

Recommendation 21

Halifax Water should reduce the number of users with domain administrator privileges to a small number who require this level of access for their jobs.

Management Response

Management agrees. This has been completed.

Contact Information

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4

Phone: 902 490 8407
Email: auditorgeneral@halifax.ca
Website: www.hrmauditorgeneral.ca
Twitter: @Halifax AG