Quantum-Safe Canada

Quantum-Safe Training for Critical Infrastructure Regulators

1. Background

The impending Bill C-26, "enacts the Critical Cyber Systems Protection Act to provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety and that are delivered or operated as part of a work, undertaking or business that is within the legislative authority of Parliament."

Proposed within the Bill is the requirement that "designated critical infrastructure operators establish a cyber security program in respect of its critical cyber systems and include in the program reasonable steps to, in accordance with any regulations;

> (a) identify and manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and services;
> (b) protect its critical cyber systems from being compromised;
> (c) detect any cyber security incidents affecting, or having the potential to affect, its critical cyber systems;
> (d) minimize the impact of cyber security incidents affecting critical cyber systems; and
> (e) do anything that is prescribed by the regulations."[1]

Consequently, those individuals charged with federal regulatory oversight and administration must be able to determine if organizational cyber security risks are effectively managed and that critical cyber systems are protected as prescribed by the regulations.

Of increasing concern is the quantum threat to Canadian critical infrastructure (CI). Many critical infrastructure organizations are only now starting to come to grips with the impending threats and may not yet fully appreciate the technologies and processes that need to be in place to address them. Similarly, those mandated to provide oversight, administration or assessment of federally regulated private-sector critical infrastructure may not yet have sufficient understanding of Q-S requirements to conduct an appropriate review of a designated operator's approach to addressing quantum threats.

There does exist Q-S expertise within the federal government, even though quantum-safe (Q-S) standards have not yet been formalized. For example, the Canadian Centre for Cyber Security has the technical expertise and authority to provide Q-S advice and guidance to critical infrastructure but is not mandated to set requirements in a regulatory or policy role. The Cyber Centre publishes Q-S recommendations (e.g. ITSAP.00.017), engages with critical infrastructure, and will provide input cyber security programs under the framework proposed in Bill C-26. However, the Cyber Centre has limited

[1] The quotes are drawn from Bill C-26 at first reading retrieved at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading on 23 October 2022.

resources at their disposal to address the national need and cannot be expected to take over the regulators' jobs.

The regulator training provided in this document is therefore critical to help mobilize essential knowledge of quantum threat, risks and mitigations to designated CI operators within the sectors subject to Bill C-26.

2. Purpose

This document outlines the Q-S training program that provides needed knowledge and skills for those responsible for the administration, oversight and assessment of cybersecurity compliance of CI operators designated by Bill C-26. Understanding that all sectors are under threat, the training has been designed so that it could be readily adapted to include other CI sectors as required.

3. Primary learning audience

The primary learning audience is individuals (federal employees, contracted resources, or federally approved contractors) who are responsible for the administration, oversight and/or assessment of compliance of designated operators of Canadian critical infrastructure under the *Critical Cyber Systems Protection Act*. They are diverse and serve in various positions across the federal public service, but are primarily working within the following ministries and agencies:

- Office of the Superintendent of Financial Institutions
- Industry Canada
- Bank of Canada
- Canadian Nuclear Safety Commission
- Canadian Energy Regulator
- Transport Canada

4. Learning requirements

Individuals within the primary learning audience work in different business and regulatory contexts. However, much of the work to support cyber security compliance regimes is similar and based upon common CI cyber threats and risk.

4.1 Knowledge and Skill Gaps

As the primary learning audience is already employed in roles where they administer and / or assess compliance within their sectors, they are assumed to have required competencies to support their current sector-based compliance functions. Accordingly, the primary knowledge and skill gaps relate to:

- Lack of knowledge on the application of Bill C-26 to their sector

- Lack of knowledge on CI cybersecurity relative to their regulatory context (although not all potential learners will necessarily lack this knowledge)
- Lack of knowledge of quantum threats and the potential cyber risks posed to their CI sector
- Lack of knowledge of the people, processes and technologies required to support Q-S cybersecurity within their assigned CI sector

4.2 Learning Outcome and Objectives

Given the variety of work and CI contexts, the primary outcome of the learning is that the learners *must be able to integrate Q-S requirements into the broader cybersecurity compliance review within their assigned sector.* This is critical to ensuring that designated CI operators also address the impending quantum threats.

Based on this outcome, the learning objectives identified for the proposed training are:

- *Define the cybersecurity context for their sector*
- *Describe key components of Bill-C26 as they relate to CI cybersecurity*
- *Identify sector-based Q-S requirements for designated operators to maintain compliance*
- *Situate the quantum threat and Q-S practices within the CI cybersecurity landscape*

4.3 Training design

The learning needs analysis and high-level design was reviewed by subject matter experts at the Canadian Centre for Cyber Security (The Cyber Centre). The training design in the Annex integrates the Cyber Centre's feedback and proposes a three-day workshop format that combines both a general perspective on cybersecurity within critical infrastructure while allowing participants to apply learned concepts and processes within a self-selected case from their own work context.

For those not yet employed within a CI context or not wishing to use an existing case, a case study is provided. This case study is intentionally drawn from a critical infrastructure context that is not covered under Bill C-26 to encourage exploration of cybersecurity requirements within an unfamiliar context and to not create preconceived notions of compliance requirements for their particular context. Trainers/ facilitators should feel free to introduce their own cases provided they support the intended outcomes.

Annex and Appendix (see following pages)

Annex – Regulator Training for Q-S Compliance
Appendix – Critical Infrastructure Cybersecurity Case Study

Annex – Regulator Training for Q-S Compliance

The following is a high-level design for a 3-day workshop to support regulator training in response to the requirements in proposed Bill C-26. Quantum-Safe Canada can readily adapt the objectives and design if amendments are made to the Bill as it moves to Royal Assent.

Intended learners: Individuals responsible for oversight, administration or assessing cybersecurity compliance as identified in Bill C-26 regulated sectors

Learning outcome: Upon completion of this workshop, participants will have the knowledge and skills to be able to construct a cybersecurity compliance matrix for their sector and conduct a compliance review.

Learning objectives:

1. Define the cybersecurity context for their sector
2. Describe key components of Bill C-26 as they relate to critical infrastructure (CI) cybersecurity
3. Identify sector-based Q-S requirements for designated operators to maintain compliance.

High-level design: A high-level design for a 3-day workshop to support regulator training is provided in Table 1. The instructional strategy includes interactive lecture, facilitated discussions, sector-based independent case study, group activities and exercises.

Assessment strategy: Formative assessment will be provided by the assigned facilitator during interactions with participants as well as during activities and exercises. Summative assessment consists of:

- a final exercise where participants will develop a compliance matrix for a given CI organizational scenario; and
- individual case study presentation subject to peer and instructor review.

Pre-requisite requirements:

1. Participants have been selected for or are employed within a federal CI regulator – while designed to support implementation of Bill C-26 regulators that are not included in Bill C-26 are also welcome to attend.
2. Pre-reading handout to include:
   - Bill C-26 or (after Royal Assent) the *Critical Cyber Systems Protection Act* and pertinent portions of the newly amended *Telecommunications Act.*
   - Security considerations for critical infrastructure (ITSAP.10.100)

- The Regional Resilience Assessment Program
- The Canadian Cyber Security Tool
- Other federal government assistance and support (Public Safety, CSIS, CSE and the Cyber Centre, RCMP, ISED, applicable federal regulators).

3. Select an organizational case study from the sector in which you are working. That case study must:
   - Be a critical infrastructure (CI) organization
   - Be dependent on some level of internet-connected operations - it need not necessarily include internet connectivity to OT or ICS; however, there must be internet connectivity to support CI operations.
4. For those not yet employed within a CI / compliance context, a CI case has been provided in the Appendix.

Facilitator Requirements: Given the subject matter, the facilitator should be cybersecurity professional who has:

- 3-5 years' experience in advising / guiding organizational cybersecurity in different technical and business contexts including critical infrastructure environments
- Demonstrates how quantum computing contributes to the cyber threat and risks to CI organizations
- Demonstrates understanding of the interrelationships between government departments / agencies and industry particularly with respect to critical infrastructure operators
- Experience in instructional facilitation on technical and non-technical topics with diverse audiences

Resource Requirements: In addition to the pre-requisite requirements for in-person or virtual delivery:

- Presentation platform or physical facility
- Breakout rooms for group activities (if required/desired)
- Collaborative tools to support group activities (whiteboards, flipcharts, etc.)
- Updated versions of Bill C-26 (electronic or print should be available depending on delivery mode)

Table 1 – High-level design for a 3-day workshop

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
1	***Module 1 - Define the CI cybersecurity context for their sector***.	1.0	**Course introduction** (10 mins) - Facilitator introduction - Workshop overview - Objectives. **Participant introductions** (30 mins).	Participants are to provide a brief (1 min) summary of their role, experience and expectations for the program (the expectations should be revisited at the conclusion of the training).	0830-0915

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
			Module 1 overview (5 mins).	The participants should be divided into reasonable sized groups (5-8) to support discussion during activities.	
			Facilitated discussion - CI context and available assistance and resources.	What does the cybersecurity of the critical infrastructure look like? (Garner perspectives and provide feedback). What resources are you aware of? (Participants will have been introduced to these organizations within the pre-reading, so this should be a review and consolidation of that information). - Canadian Centre for Cyber Security ▪ CI Cyber Security Guidance ▪ National Cyber Threat Assessment ▪ Cryptographic standards ▪ Industry collaboration - Public Safety ▪ CI guidance ▪ CI gateway ▪ Cyber and resilience assessments ▪ CI partners - Innovation Science and Economic Development ▪ Canadian Forum for Digital Infrastructure Resilience (CFDIR) - RCMP ▪ Critical Infrastructure Intelligence Team (CIIT) ▪ Federal Policing (Cybercrime) ▪ National Security Information Network - Canadian Security and Intelligence Service (CSIS) ▪ Integrated Threat Assessment Centre ▪ Info on espionage and foreign interference	0915-0930

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
				- National Institute of Standards and Technology (US) and Cybersecurity - Critical Infrastructure Security Agency (US)	
		1.1	**Lecture -** Inventory critical assets.	Definition of critical assets based on risk - Tangible value (replacement cost, business cost, etc.) - Intangible or unassessed value (reputation, public trust, intellectual property, etc.) - Confidentiality, integrity and availability. Asset inventory development process - System and data mapping - Critical asset assessment.	0930 - 1015
		Break			1015-1030
			Case study – identify CI critical assets.	Participants will select an organizational case from within their sector and, using guidance provided, identify the primary CI critical assets (3 or 4 assets upon which the organization relies). This can be done in groups if the audience make-up allows. Reserve five minutes for debrief.	1030-1100
		1.2	**Lecture -** Identify primary CI threats.	CI exposures (with relevant examples): - Physical - Digital/IT - Human - Supply chain. CI current and emerging threats: - Primary threats to CI with relevant sector examples (from National Cyber Threat Assessment) - Emerging threats: ▪ AI / ML ▪ Cloud / Edge / IoT ▪ Quantum.	1100-1130

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
			Case study - identify cyber threats to CI operations including emerging threats.	Based on their existing case and using guidance provided, participants will identify the primary threats and risks to the organization. This can be done in groups if the audience make-up allows. Reserve five minutes for debrief.	1130-1200
		Break			1200-1300
		1.3	**Lecture** - Define CI impacts and cyber risks.	Definition of cyber risk (a.k.a. digital risk) – risks to organizational systems and information arising from cyber threats. Translating cyber risk to organizational risk (cyber threats that create cyber risk that, in turn, will have operational, legal, compliance, strategic, financial impacts that create organizational risk).	1300-1330
			Facilitated discussion - Impacts using scenario-based examples.	Leverage participant experience to discuss potential cyber threat scenarios and impacts for their CI contexts.	1330-1345
			Activity - Threat and risk assessment overview and exercise.	Conduct a brief walk-through of the threat and risk assessment. Using a generic template, have participants identify cyber threats and risks for their CI case. This can be done in groups if the audience make-up allows. Reserve five minutes for debrief.	1345-1415
		Break			1415-1430
			Case study – Translate cyber risk to organizational risk.	Using their ongoing case and the threat and risk assessment information, have participants translate cyber risks into specific organizational risks within their CI context (operational, legal, compliance, strategic, financial). This can be done in groups if the audience make-up allows.	1430-1530

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
				Reserve five minutes for debrief.	
		1.4	Review and summary.		1530-1600

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
2	***Module 2 - Describe key components of Bill C-26 as they relate to CI cyber security***.	2.0	**Module 2 overview**.	Brief review of Module 1. Facilitated discussion on implications of Bill C-26.	0830-0900
		2.1	**Lecture -** Definitions and authorities.	Definitions and authorities identified in the Bill: - Governor-in-Council - Ministerial responsibilities: ▪ Superintendent of Financial Institutions ▪ Minister of Industry ▪ President of the Bank of Canada ▪ President of the Canadian Nuclear Safety Commission ▪ Chief Executive Officer of the Canadian Energy Regulator ▪ Minister of Transport. - Designated operators – classes and regulator.	0900-0930
		2.2	**Lecture -** Regulator responsibilities.	Regulator roles related to oversight, administration and assessment of federally regulated operators. Interactive discussion that engages participants identifying with a specific role and their potential responsibilities.	0930-1000
			Facilitated discussion – Regulatory responsibilities and eco-system.	Leverage participant experience and roles to discuss the various government and industry supports for them fulfilling their responsibilities related to operator cybersecurity compliance. Refer back to the supports and resources introduced in module 1.	1000-1015
		Break			1015-1030

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
		2.3	**Lecture** - Compliance requirements.	Deconstructing the requirements of Bill C-26 to include: - Cybersecurity program requirements - Mitigation of third-party and supply chain risk - Reporting requirements - Compliance agreements and measures. Use questioning to confirm participants knowledge of the key components of the Bill as it pertains to their roles.	1030-1130
			Facilitated discussion – Compliance and risk.	Referring back to key points on exposures and translating cyber risk to organizational risk, engage participants in a discussion on the differences between cybersecurity compliance and broader risk management stressing that compliance does not necessarily mean that all organizational cyber risk has been effectively managed.	1130-1145
		2.4	**Review and summary**.	Review module 2 objectives. Confirm key points with participants.	1145-1200
		Break			1200-1300
	Module 3 - Identify sector-based quantum-safe (Q-S) requirements for designated operators to maintain compliance.	3.0	**Module 3 overview**.	Brief review of how module 1 and 2 contribute to module 3.	1300-1305
		3.1	**Lecture** - Situating quantum. threats and risks within CI.	Overview of quantum computing and threats to CI - Differentiating between classical and quantum-safe cryptography - Defining crypto agility - Assessing impacts on current cryptographic technologies and processes, including public key infrastructure - Identifying audience relevant IT, OT, IoT, and supply chain examples Overview of the quantum risk assessment process that organizations should include in their cybersecurity assessment.	1305-1330

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
			Case study - Identify quantum threats to the CI organization.	Using their ongoing case, the previous understanding of cyber risks and awareness of quantum threats, participants are to define the potential quantum threats to CI for their case. This can be done in groups if the audience make-up allows. Reserve five minutes for debrief.	1330-1400
		Break			1400-1415
		3.2	**Lecture -** Q-S organizational processes and technologies.	Migration process and timeline to a safe and secure post-quantum crypto environment. Q-S best practices within an organization noting that these will need to be adapted to the CI context and the unique systems and processes of each designated operator. Key planning activities: - Quantum risk assessment - Migration strategy development to meet the quantum threat timeline - Establishing current cybersecurity posture - Conducting quantum risk assessment - Identifying priority risks and mitigations based on industry standards and compliance requirements ▪ Third party and supply chain considerations - Allocating resources and investments to meet quantum-safe timeline requirements. Key integration activities: - Testing – acceptance and integration - Updating policies, plans, processes and procedures	1415-1515

Day	Objective	Module	Learning element	Content details and facilitator instructions	Timing
				- System manager and technician training. Key implementation activities: - Monitoring implementation of Q-S processes and technologies - Introduction of updated policies, plans, processes and procedures - User training as required. Ongoing management requirements: - Measuring, monitoring and incident response - Maintenance of Q-S capabilities throughout their lifecycle.	
			Facilitated discussion – integration Q-S practices into cybersecurity activities.	With the context associated with migration to a Q-S environment, discuss the potential challenges facing CI organizations such as: - The implications of organizational size and structure - Legacy systems - Technical maturity - Level of dependence on third-party services.	1515-1545
		3.3	**Review and summary.**	Review module 3 to date. Confirm key points with participants.	1545-1600

Day	Objective	Module	Learning element	Content details and facilitator instructions	Time
3	***Module 3 (continued) - Identify sector-based quantum-safe (Q-S) requirements for designated***	-	**Module 3 (first part) review**	Review previous day's highlights	0830-0840
		3.5	**Lecture -** Compliance requirements and Q-S.	General Q-S requirements to maintain compliance including: - Overview of Q-S conformance and testing protocols - Regulatory and compliance requirements - Industry standards with audience relevant examples	0840-0910

Day	Objective	Module	Learning element	Content details and facilitator instructions	Time
	operators to maintain compliance			- Queries into organizational practice and actions that can be used to assess Q-S requirements needed to support compliance such as: ▪ Have they established plan with a timeline that sufficiently prepares them for the anticipate quantum-threats? ▪ Are they aligning actions to relevant standards? ▪ Do they maintain awareness of developments in Q-S processes and technology? ▪ Do they have a training program that provides employees with required Q-S knowledge and skill? ▪ Do they have a strategy to address Q-S post evolving PQC security requirements, lifecycle management and forward-compatibility for Q-S processes and technology?	
		3.6	**Lecture** - Integration of Q-S requirements into compliance	Integrating Q-S requirements into cybersecurity program while ensuring compliance.	0910-0920
			Group exercise – Complete cybersecurity compliance matrix (to be based on final Bill).	Participants are to construct a cybersecurity compliance matrix for their CI context that includes Q-S requirements. Where uncertainty exists, a 'question to the experts' can be inserted rather than an explicit Q-S requirement. Reserve five minutes for debrief.	0920-1000
		Break			1000-1015
		3.7	**Case Study** – Identifying comprehensive compliance requirements.	Using their ongoing case study, participants will identify compliance requirements for their CI cases to include integration of Q-S practices. As they may	1015-1200

Day	Objective	Module	Learning element	Content details and facilitator instructions	Time
				be unfamiliar or uncomfortable identifying specific compliance requirements in an unfamiliar context, they can alternatively develop questions that relate to the potential cybersecurity and Q-S actions that should be taken. Participants are to develop a short executive-level brief of their case organization's compliance requirements / questions. They should be prepared to answer questions of what they might be looking for as evidence of compliance.	
		Break			1200-1300
		3.8	**Participant briefs.**	Each participant provides a 2–3-minute executive-level brief of their case and the identified compliance requirements. Peers and facilitators should provide feedback and query what evidence of compliance is required.	1300-1500
		3.9	**Review and conclusion.**	Review of objectives, content and key points from the training. Embed learning confirmation (e.g., questions) into the process. Review of participant expectations from Day 1 introduction. Completion of training-evaluation forms and discussion of any feedback.	1500-1600

References and resources

Canadian Centre for Cyber Security (2019). Preparing your organization for the quantum threat to cryptography (ITSAP.00.017), https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

Canadian Forum for Digital Infrastructure Resilience (CFDIR) (2021). Canadian national quantum readiness: Best practices and guidelines, https://quantum-safe.ca/wp-content/uploads/2022/01/CFDIR-Prati-Tech-Quant-EN.pdf

Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, 176, 99-118.

Canada (2022). Bill C-26 - An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, (First Reading, June 14, 2022). https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading

ISO/IEC (2013). ISO27001- Information Security Management, https://www.iso.org/isoiec-27001-information-security.html

Mosca, M., Piani, M. (2021). Global Risk Institute, Quantum Threat Timeline Report, 2020 https://globalriskinstitute.org/download/quantum-threat-timeline-report-2020/

Mosca, M., Mulholland, J. (2017). A methodology for quantum risk assessment: Technical report. Global Risk Institute, https://globalriskinstitute.org/publications/3423-2/#:~:text=Quantum%20Risk%20Assessment%20Methodology,threats%20are%20likely%20to%20emerge

NIST (2022). Cybersecurity Framework, https://www.nist.gov/cyberframework

NIST (2022). Cybersecurity and Privacy Reference Tool (CPRT), https://csrc.nist.gov/projects/cprt

NIST (2021). Getting ready for post-quantum Cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms, A NIST White Paper, https://doi.org/10.6028/NIST.CSWP.04282021

NIST (2022). PQC, https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST (2022). Post-Quantum Cryptography Standardization, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

NSA (2021). Quantum computing and post quantum cryptography FAQ, https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQ-S_20210804.PDF

Quantum-Safe Canada (2021). Organizational migration to quantum-safe cryptography: A role-based framework, learning outcomes and curriculum model,

Technation (2019). Canadian Cybersecurity Skills Framework[2], https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/

[2] The Canadian Cybersecurity Skills Framework was the basis for the Cybersecurity National Occupational Standard which is currently in final review at the CIO Strategy Council. The Standard in development includes the Q-S tasks and competencies for each major cybersecurity role. Once published, this Standard will supersede the information in the Canadian Cybersecurity Skills Framework.

Appendix – Critical Infrastructure Cybersecurity Case Study

Purpose

This case study is provided to support activities embedded within Quantum-Safe Training for Critical Infrastructure Regulators. It is primarily provided for those who are not yet employed within an existing critical infrastructure (CI) context or those not wishing to use a case from their current contexts.

This case study is intentionally drawn from a critical infrastructure context that is not covered under Bill C-26 to encourage exploration of cybersecurity requirements within an unfamiliar context and to avoid creating preconceived notions of compliance requirements for their particular context.

Case Introduction

You are the compliance officer within the Natural Resources Canada (NRCan), responsible for initiating compliance assessments of water treatment and distribution facilities that fall under federal jurisdiction. NRCan has been conducting cybersecurity related training and voluntary assessments for a number of years. With the increased cyber threats against Canadian critical infrastructure, they have been looking at rolling out a compliance regime as well and so have been including more rigour so as to align their assessments with Bill C-26. Your current task is to conduct a voluntary cybersecurity compliance assessment of a water treatment facility which is owned and operated by a public utility under contract to the Crown.

The public utility has several similar federal, provincial and municipal contracts and are members of the Canadian Water and Wastewater Association. In this case, the utility has a local branch in a remote location that is responsible to treat water from the local watershed so that it is suitable for human consumption. The treated water is also used for a variety of other purposes such as fire control and private sector / commercial use to minor industries. The public utility also serves a large mining community as well as several power generation facilities which rely upon the water for continued operations.

While they are serving a remote community under federal jurisdiction, the utility has been collaborating with the local municipal authorities on improving effectiveness and efficiency of water treatment practices. They have previously met all water treatment compliance requirements and appear to have a good record in reporting and responding to observations. However, they realize that none of the local water treatment plants have invested a great deal of effort in addressing cyber threats. The primary reason for this is that they believe that they are an unlikely target given their remote location and limited population served.

Organization

While the large public utility is responsible for the overall operation of the water treatment site, there is a local team led by a Managing Engineer, a fluid engineer, who reports to the Regional Office in Scarborough, Ontario who has been identified as the liaison for your upcoming cybersecurity compliance assessment. The Managing Engineer is a member of the Water Environment Association of Ontario and is has become a strong advocate for safe water treatment practices in Canada. The Managing Engineer is assisted by a junior biochemist (intern), two fulltime water-treatment technicians,

and three regular administrative staff. Efficiencies resulting from technological improvements have resulted in them cutting two water-treatment technicians from the local team who have been moved to other locations. There is IT support from the headquarters as required, though one of the administrative staff considers themselves to be a bit of a 'techie' and helps ensure that the office is up to speed on IT related matters.

IT and Digital Infrastructure

As a result of the recent pandemic, the local office implemented remote work practices so employees could work from home. While the headquarters indicated that they would fund acquisition of laptops for employees, they also gave the employees the option of using their own home systems and get reimbursed for internet fees and any software requirements. They demanded, however, that employees sign a policy that indicated that they would have security software installed (firewall and anti-virus).

While the majority of employees have returned to office full-time, they still find efficiencies in allowing administrative employees the opportunity to work from home 1-2 days per week. Accordingly, they are typically sending work from the office to their home systems on a regular basis. While there aren't many sensitive files, employees understand that any sensitive files should be sent via encryption to their home systems.

Until the pandemic, the office was still using Windows 7 that was downloaded onto a local server. They struggled with updates and functionality over the past couple of years. So, they happily replaced this with Microsoft O365 to support all administration activities including local account administration, employee management, email as well as database management using the associated Microsoft applications (Word, Excel, Outlook, etc.). They use OneDrive to support all file management and back ups. The O365 licence is managed through the headquarters, but the local office gets all updates directly from Microsoft.

The utility has a Supervisory Control and Data Acquisition (SCADA) system in place that is used to manage, monitor and log operational processes related to water treatment, storage and distribution. As they have been reduced by one technician, they are unable to establish 24/7 in-person monitoring, and recently adopted SCADA monitoring and management through IoT devices (adapted cellular phones). These devices include the monitoring and alerting software through a direct, encrypted channel to the local server and monitoring workstation that also connects to the SCADA system.

They realize that they have not kept pace with the cyber threats, that there are a number of improvements that they need to make. Anticipating that their industry will soon also be subject to legislative compliance, they have been looking at what policies, processes and procedures they might need to put in place to ensure organizational security as well as the safety and security of local systems.

Questions

With your understanding of Bill C-26 and the potential compliance requirements for critical infrastructure, use that information as you consider safety and security of water treatment infrastructure.

Threats and risks

What are the potential threats and risks to this critical infrastructure?

What are supply chain risks are there? What other supply chains are they part of that may also be critical?

Have emerging technologies and related threats been considered – Quantum, AI, etc.?

What additional threats will quantum computing pose and what could be the impacts?

Security actions

What organizational security controls are in place? Are they sufficient to meet the existing threats?

What steps have they taken to address security as they move to remote operations?

What level of planning have they conducted to address future threats including quantum-threats?

To what degree have they investigated Q-S standards?

Have they implemented cybersecurity training and awareness? Do they anticipate including Q-S knowledge and skill requirements in their training?

Future Proofing

How is the organization structure to address cyber threats now and in the future?

Do they maintain awareness of developments in Q-S processes and technology?

Do they have a strategy to address Q-S post evolving PQC security requirements, lifecycle management and forward-compatibility for Q-S processes and technology?

Overall Assessment

If this critical infrastructure was subject to Bill C-26, how well would they meet the compliance requirements?

What would be your key recommendations to the Managing Engineer concerning their cybersecurity posture?