Quantum-Safe Canada

CYBERSECURITY RESEARCH LAB

QUANTUM-SAFE TABLETOP EXERCISE: SENIOR LEADER'S HANDOUT

Purpose

Welcome to the Quantum-Safe Tabletop Exercise. This document contains the agenda and handouts that relate to the exercise.

Feel free to use this handout to take notes throughout the exercise.

Agenda

0915-0930	Introduction and expectations
0930-1130	Exercise (including a break)
1130-1200	Debrief and feedback
1200-1300	Networking and lunch

Definitions

Cryptography	The process of **making plain information unreadable, as well as to convert it back to a readable form**. This includes constructs such as encryption, digital signatures, hashing, etc. that are used to authenticate the source and protect the confidentiality and integrity of information within and across a variety of information and communications technologies.
Cybersecurity	The **protection of digital information and the infrastructure on which it resides**. More specifically, cybersecurity includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.
Deliberate cyber threat	A cyber threat actor who, using the internet, takes advantage of a known vulnerability for the purposes of **exploiting a network and the information the network carries**.
Encryption	**Converting (encoding) information from 'plaintext' to 'ciphertext'** to hide its content and prevent unauthorized access or manipulation.
Quantum computing	Exploits quantum properties to store and manipulate information that enables mathematical, optimization, and search problems **much faster than conventional computers.**
Quantum threat	Quantum computers used in ways that **can break or weaken widely used cryptographic schemes**.
Quantum-safe cryptography	The use of new cryptographic tools, whether conventional or quantum in nature, designed to be **resistant to quantum attacks**.
Quantum-safe	A state of an information system where **quantum threats have been mitigated** through either traditional or new quantum-safe practices, processes and technologies.

Handout 1 – Initial article

Is your business ready for the quantum threat?

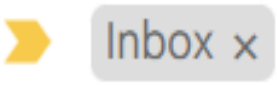
While experts have yet to agree on exactly when the quantum threat will be realized, conservative estimates hover around 15 years. Many experts suggest, however, that it could be considerably sooner given the level of investment and innovation within certain nation states and the private sector.

Organizations are urged to identify quantum vulnerable systems, evaluate what is at risk and start planning for the eventual threats.

- What information systems or data do you have that rely on quantum vulnerable cryptography and encryption?
- What exposures or risks are there to quantum threats?
- As the threat is 15 years out, what are your immediate concerns if any?

Handout 2 – Internal email

Quantum Readiness



To: CIO <CIO@yourorg.ca>

Good day. I had a discussion with a colleague at an annual IT conference and they showed me a recent notice from the Canadian Centre for Cyber Security on the quantum threat. After reading it, I did a quick assessment of our cybersecurity posture.

While the threat from actual quantum computing may be 15 years out, I am quite concerned about the level of investment we'd need to prepare for the quantum threat. Perhaps we can talk about this before your next Executive Group meeting to see if we can get some in-year funding for the assessment and planning.

Director, IT Architecture

Reply Forward

- What is your initial response to this request?
- What types of investments do you think might be required to support initial migration to a quantum-safe (Q-S) environment?
- What expertise do you have access to?

Handout 3 – CIO Briefing

"In addition to the investment to address future quantum risks, there is a more pressing issue that I realize that we haven't yet discussed. There is a threat known as 'harvest now, decrypt later' that cybercriminals may employ. This involves threat actors hacking into our current systems and taking encrypted data now with the intention of decrypting it once the quantum capability exists. I'm not fully familiar with all the data we have, but I'm thinking that this could be a problem."

- What are your first thoughts about this type of threat?
- What data or information do you currently have that may pose a risk if exposed in the future?

Handout 4 – Q-Bit Times Article

The Q-Bit Times

High-tech news direct to your inbox on digital parchment

Breaking News - The tech world has been rocked with the recent statement by a medium-sized technology firm that indicated that they are confident that they will have commercially viable quantum capability within the next five years. While many have their doubts and suggest that this is an attempt to attain more investment, government officials have assessed the evidence and agree that quantum computing could be a reality sooner than we thought.

- How does this change your plan?
- What should be your first steps?

Handout 5 – Future News Article

It's a quantum-world: Canada's only 24-hour quantum-focused online news source

2026 - The state of quantum-computing in Canada: How are businesses fairing on preparing for the emerging threat?

It's been a few short years since we announced how businesses should be preparing for the quantum threat. Despite this, a recent survey indicated that less than 50% of businesses have taken the minimum actions required to protect their systems and data from what will soon be available to those who can afford it - a quantum-capable computer.

We interviewed a cybersecurity specialist who stated, "we simply don't have enough qualified people to meet the demand - we have client requests and commitments that already reach out five years and now it looks like the government is going to legislate action in some cases. So, some of our existing clients may be plumb out of luck."

Having watched the cybersecurity challenges over the past two decades, it should be no surprise that some companies will simply not be prepared. The key question is, ***would they survive a quantum attack?***

Selected Resources

Canadian Centre for Cyber Security, (2021). 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) (2022). Canadian National Quantum-Readiness: Best Practices and Guidelines. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/cfdir-quantum-readiness-best-practices-v02-en.pdf

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

Mosca, M., Piani, M. (2022). Quantum Threat Timeline Report, Global Risk Institute. https://quantum-safe.ca/wp-content/uploads/2023/01/2022-quantum-threat-timeline-report-dec.pdf

National Institute of Standards and Technology (NIST) (2022). Post-Quantum Cryptography. 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

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

Contacts

Bill Munson
Managing Director
Quantum-Safe Canada
bill.munson@quantum-safe.ca

Dr. Atty Mashatan
Canada Research Chair & Director, Cybersecurity Research Lab
Toronto Metropolitan University
amashatan@torontomu.ca

Dr. Randy Purse
Consultant
Quantum-Safe Canada
edward.purse@gmail.com