Quantum-Safe Canada

Quantum-Safe Training – Leadership Series

Technical advisor and senior technical manager (TTX)

Table of Contents

Published by:
Quantum-Safe Canada
31 March 2023

Purpose and Applicability

This guide supports cybersecurity and management professionals in tailoring and facilitating tabletop exercises for organizational decision makers that may include:

- Technical advisors (CIOs, CTOs, CISOs, etc.)
- Senior technical managers (IT or OT)
- IT managers and team leads
- OT managers and team leads
- Technical teams, e.g., IT, OT or security teams that are responsible for defining cyber threats and mitigations

The tabletop exercise features a progressive quantum-threat scenario intended for technical managers to aid them in identifying quantum threats to digital systems and data, technical implications and potential mitigations to support quantum-safe (Q-S) migration.

This guide should not be provided to participants. Rather, they should be provided with links to the selected resources at the end of this guide.

TTX Tailoring and Preparations

A TTX can have many goals and support different functions. It can be used to:

- Educate or train participants
- Support short, medium or long-term planning and preparations
- Assess processes and procedures
- Evaluate communications and workflows
- Help solve complex problems.

This guide provides a framework for the conduct of a TTX based on a quantum-threat scenario that is intended to both educate and support technical planning and Q-S migration. The client or groups of clients may have additional goals or outcomes of that could be scoped within the TTX.

This TTX is generic in nature so that elements such as exercise foreground and injects can be adapted to suit a particular sector, industry or business environment as well as a public, private or non-profit organizational context.

If tailoring is required, the facilitator should:

- Define the target audience – Who are the participants and what roles they fill within the organization(s)? The TTX can apply to senior technical advisors (CIO, CTO, CISO), senior IT / OT managers, technical team leads, or the teams comprised of IT, OT or technical security personnel.
- Identify client goals and outcomes – Why does the client want the TTX and what do they wish to achieve or learn from the TTX?
- Determine any specific parameters for the TTX – What are the potential client or delivery constraints? This includes the media used, timeline, location, scenarios, known issues, or processes to be assessed.
- Establish the current state of the organizational processes – What is the organization's general cybersecurity posture and maturity? This will help define both the goals and the elements required in the TTX that will enable discussion and feedback.

Prior to delivery of the TTX, the facilitator should:

- Adjust the scenario to address client goals
- Add, delete or amend injects to support the scenario
- Check timely insertion of injects and the overall TTX timing
- Create or amend visual aids that are needed to support the TTX
- Conduct a dry-run of the TTX to ensure that it flows well and meets the time requirements.

TTX Roles

Facilitator - The facilitator should be a technically savvy cybersecurity professional who is familiar with quantum threats and risks, has a general understanding of quantum-safe strategies, technologies and processes and knows how cryptographic systems and encryption are commonly used in support of organizational cybersecurity. As well, they should have a comprehensive understanding of cybersecurity best practices and the types of technical and non-technical security controls that may help mitigate current and future quantum threats. Finally, they should be experienced in risk management and cybersecurity planning activities.

Participants – Depending on the TTX goals, participants may contribute to the TTX discussions in their current role, an anticipated role or an assigned role. As the intent of this TTX is to support organizational Q-S migration, participants should:

- Play their own or assigned role
- Take the scenario at face value

- Be encouraged to 'think aloud,' describe their thought process and disclose assumptions behind decisions or proposed actions.

Observers – While the facilitator will be guiding the exercise, the client may wish to have observers for the TTX. These observers can provide some objectivity and support critical analysis as the TTX unfolds. They can also offer their observations and insights during the debrief and any follow up actions.

Master Event List

The Master Event List (MEL) is a chronological representation of facilitator-led actions (injects) to prompt participant activity and discussion. It ensures that events happen in a sequence that will support achievement of the TTX objectives. In addition to the injects, the facilitator may include expert commentary or ask questions about the situation or context that support participant learning and decision making.

This TTX is planned for a duration of two hours from initial introduction to debrief including 15 minutes for introduction, a 10-minute break mid-exercise and 15 minutes for debrief. Depending on the organizational goals, added elements, and discussions, the TTX could be extended. However, given the general goal of this TTX, the intensity of the activity, and the potential target audience, it is recommended that the exercise not exceed three hours.

The MEL below is tailored to a quantum-threat scenario that includes an initial timeline based on a conservative estimate of when organizations are likely to experience a cryptographically relevant quantum threat. At mid-exercise, the timeline is accelerated, and the threat is realized several years earlier. This is intended to help demonstrate the uncertainty of the threat timeline and support contingent planning and preparation. The injects / activities are designed to be supported by a presentation or discussion guide with example correspondence, articles and other simulated materials which should be labelled as 'for exercise only'.

Timing (mins)	**Inject / Activity**	**Topics/content**	**Suggested discussion points**
0000-0015	Introduction	Personal introductions Goals of the exercise Ground rules for the exercise Initial scenario read-in Critical definitions:	

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		• Quantum risk • Quantum threat • Quantum-threat timeline • Cryptographically relevant quantum threat • Q-S migration • A Q-S technical environment	
0015	Exercise starts		
0015-0025	CEO inquiry email	"Good day, I'm not sure about how up to speed you are on the potential of a quantum threat. I just read this article and I'll send it to you if you want. At any rate, I guess this is going to be a problem within the next 15 years or so. I know this is quite a few years out yet. However, I need to understand the longer-term implications and also need to inform the Board if there are going to be significant costs that we need to account for. I'd like you to put together a short brief on our current cybersecurity posture and what we might be looking at to ensure that we understand the future risks." The CEO has some $ allocated to get some initial expert perspective on this.	As the potential threat is 15 years out, what are our first reactions to this? Where would you start? Possible responses: - Get a better appreciation of the 'urgency' given the timeline - Learn more about the quantum threat and quantum risks - Expertise / internal capability - Asset inventory - Cybersecurity assessment What information systems or data do you have that rely on quantum vulnerable cryptography and encryption?
0025-0035	Initial consultation report	A cybersecurity expert you consulted provided you with an initial assessment in which the key points are:	What are your concerns now?

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		- 15 years is a stretch it could be far earlier - All PKI/asymmetric key are potentially at risk - NIST is defining Q-S standards upon which a vendor list will be based - There is an additional threat of 'harvest now/decrypt later' that you should consider - They can do the quantum-risk assessment and provide prioritized actions	What are the initial implications of this new information? What do you think your next steps are? Possible responses: - Further research - Capability to do the quantum risk assessment - Re-assess the timeline - Addressing harvest now/decrypt later threat and what they could be doing now – what is currently at risk?
0035-0045	Board brief	Based on your informal discussion with the CEO on the pressing harvest now/decrypt later threat and the potential actions required, they've asked you to brief the Board.	What type of information do you think you'll need for this brief? What organizational data or systems may be at risk? Prompt, if needed: - sensitive information - corporate secrets - IP - Source codes - AI or control-system data channels and configurations

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
			- Digital interfaces with equipment that are protected by existing encryption What mitigations might be available?
0045 - 0060	Plan development	You have some initial mitigations for the immediate threat. Now the CEO has asked you to put together a plan to ensure that the organization is safe moving forward.	What elements do you need to consider so that you can meet the 15-year timeline? Capture key points on a screen or whiteboard. Possible points may include: - Inventory of vulnerable cryptographic systems and encryption processes including upstream and downstream supply chain - Identification and prioritization of quantum risks including those associated with attack scenarios such as ransomware, data theft and supply chain attacks - Coordination with partners / suppliers - Are third-party services also Q-S - Policy and practice changes - Q-S standards and compliance

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
			- Costs related to implementation of Q-S technologies and processes - Access to Q-S expertise - Role-based training - Incremental approach to procurement, testing, integration and installation - Lifecycle management to maintain Q-S posture
0060-0070	Break		
0070-0080	News release – Accelerated quantum threat six-months later	"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 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? Possible responses: - Review where we are in the plan and what needs to be accelerated - Verify critical quantum risks and any implications on existing compliance requirements - Identify what needs to happen to mitigate those risks - Determine what investment may be required and how we would fund it

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
			- Identity the expertise that would be needed
0080-0090	Article – state of quantum computing in Canada three years later	Excerpts from business article (three years in the future): *"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 plum 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."*	Forecasting out to this time, how do you envision your plan will unfold. What other challenges might there be over the next five years that you'll need to consider? Possible responses: - Business changes - Technology changes - Other changes to the cyber threats landscape including investment in capabilities to counter AI-enabled threats - Increasing demand for expertise / talent - Keeping the team up to speed - Ongoing investment in cybersecurity - Organizational changes that will necessitate other tech investment to stay relevant or comply with evolving standards and legislation (e.g., CI requirements, privacy, industry standards)

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
0090-0100	The future in retrospect	How would you like to see yourself and your organization once quantum-computing and related quantum threats become a reality?	
0100	Exercise completed		
0100-0115	Debrief	Having completed the exercise: What are your primary concerns? What near term actions do you think you should take? Were there any other things that you learned that you consider valuable?	
0115-0120	Feedback	How did you think the exercise went? What suggestions for improvement do you have to offer?	

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