Quantum-Safe Canada

Quantum-Safe Training – Leadership Series

Organizational Decision Maker Tabletop Exercise (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:

- Board members
- Senior executives (C-Suite)/ business owners
- Senior responsibility managers (e.g., functional areas such as finance, operations, IT, security, human resources, etc.)
- Program directors/managers
- Senior business advisors
- Other similar roles.

The tabletop exercise features a progressive quantum-threat scenario that challenges the organizational decision makers to identify quantum risks and potential mitigations within the quantum-threat timeline.

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 organizational planning and preparation. A client may have additional goals or outcomes that could be scoped within the TTX if desired.

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 do they fill within the organization(s)? The TTX can apply to a board, an executive or managerial group, a specific team, or a more diverse audience to include senior level business advisors.
- 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 senior cybersecurity or management professional who is familiar with cyber risk management, quantum threats and risks and has a general understanding of quantum-safe strategies, technologies and processes. Detailed technical knowledge is not required as the TTX activities pertain to organizational decision making, risk, planning, and appropriate allocation and/or acquisition of resources to address the quantum threat.

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.

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.

This Master Event List (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 • Quantum-safe environment	
0015	Start of exercise		
0015-0020	Current day quantum threat timeline article (if desired an actual article can be used if permissions have been granted)	Excerpts from business article (current day): *"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?
0015-0025	An email from the CIO / CTO with initial concerns	"I recently 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 about the level of investment we'd need to make to prepare for the quantum threat. Perhaps we can talk about this at the next to	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?

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		and see if we can allocate some in year funding for the assessment and planning."	
0025-0040	Role-play CIO briefing	In addition to the investment to address future quantum risks, there is a more pressing issue that I have not yet discussed. There is a threat known as the 'harvest now, decrypt later' strategy that cybercriminals may employ. This involves them hacking into our current systems and taking encrypted data now with the intention of decrypting once the capability exists. I'm not fully familiar with all of 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? (Prompt, if needed) Consider requirements that pertain to protection of: - sensitive information - corporate secrets - IP - Source codes - AI or control system data channels and configurations - Digital interfaces with equipment that are protected by existing encryption
0040 - 0050	Plan development	Considering what we've discussed, what elements would you need to consider for your migration plan to 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

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
			- 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 - Costs related to implementation of Q-S technologies and processes - Investment plan to support costs - Expertise - Role-based training - Incremental approach to procurement, testing, integration and installation - Lifecycle management to maintain Q-S posture
0050-0060	Break		
0060-0080	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*	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

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		computing could be a reality sooner than we thought."	- 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 - 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*	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: - Market changes / profit margin and ability to invest - Other changes to the cyber threats landscape including investment in capabilities to counter AI-enabled threats - Increasing demand for expertise / talent - Organizational changes that will necessitate other tech investment to stay relevant or

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		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."	comply with evolving standards and legislation (e.g., CI requirements, privacy, industry standards) - Keeping the board/clients/investors informed
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