A Methodology for Quantum Risk Assessment

Author: Dr. Michele Mosca & John Mulholland

GLOBAL RISK INSTITUTE

DISRUPTIVE TECHNOLOGY

INTRODUCTION

Until recently, quantum computing was often viewed as a capability that might emerge in some future time, almost something that properly belongs in a science fiction novel.

The science behind these computers originates in the physics of quantum mechanics, which presents a fundamental change in our understanding of the universe. The concepts can be difficult to reconcile with the world we live in; for example, in a quantum computer a bit can somehow be both zero and one at the same time! Even many physicists have had trouble with these revolutionary ideas, but experiments and observations have validated quantum theory and its underlying principles are evident in common devices such as lasers and transistors. These technologies only hint at the full promise of quantum, but considerable work is still required before we can build a true quantum computer.

This milestone is probably a decade or more in the future, but the work is being pursued by many researchers around the globe since quantum technology promises advantages in a variety of areas such as sensors, communications, optics and computation. In 1994, mathematician Peter Shor described an algorithm which enables quantum computers to solve extremely difficult mathematical problems, such as factoring very large numbers. Such problems are essentially unsolvable using today's computers. So difficult are these problems that they have become the mathematical underpinning of the most commonly used security systems on the Internet. Modern public-key cryptographic systems provide security for virtually all sensitive communications on the Internet, including banking, email and web site access.

Once effective quantum computers[1] are available, they will essentially eliminate the cryptographic strength of these public-key cryptosystems. More traditional shared-key cryptosystems (such as AES) will also be affected, reducing their effective security strength to roughly half of what we would consider it to be today.

This will have a devastating effect on the systems used to protect electronic communications and digital transactions. Most secure internet processes rely on protocols that employ public-key cryptography, including those used to secure web sites, for banking transactions, secure email and digital signatures. There are few businesses or individuals who could be confident of their cyber security profile once the quantum computing era arrives.

How do I deal with a threat that hasn't yet emerged?

Despite steady progress in the development of quantum computing, it will likely be ten to fifteen years before quantum computers become available. Perhaps this

[1] For this discussion we define a quantum computer as one with sufficient capability (superposition, entanglement), capacity (qubits) and reliability (redundancy, error correction) to efficiently execute Shor's algorithm. Efficient execution implies that solutions to factoring and discrete-log problems can be found in polynomial time, rather than the sub-exponential time required on a conventional computer.

accounts for the low level of concern among those responsible for cyber security planning and decision making. Undoubtedly their attention is focussed on the plethora of cyber threats facing all organizations today, and perhaps they feel there will be plenty of time to respond once quantum computers actually emerge.

There are several problems with this type of thinking. Once a quantum computer is delivered it will immediately affect the security of all Internet communications and data. Unless organizations are prepared for this sudden crisis, they will face an immediate need to replace their existing cryptographic security systems with quantum-safe solutions.

Adapting an organization's entire cryptographic infrastructure during a period where everyone else is attempting the same thing is likely to be difficult and expensive. Few organizations actually develop cryptographic security capabilities, most obtain them from vendors, often integrated into network or security products. Without advance preparation, an organization may have no idea of their vendors' ability to furnish quantum-safe solutions, nor knowledge of the difficulties they will face integrating the new technology into their environment. However, this is not the only problem that ill-prepared organizations are likely to face.

Several quantum-safe solutions have been proposed, but few have made it out of the research phase, and even these require much work to verify that they can resist both conventional and quantum attacks. Current cybersecurity protocols have faced real-world challenges over the past 15 or more years, and have evolved to their current state. We trust them partly based on their mathematical foundations (now being challenged by quantum), but also because they have stood the test of time. If we are to trust quantum-safe cryptography, it is important that real-world testing begin as soon as possible.

Managing this problem will require awareness, planning and preparation. A well-prepared organization can take steps to integrate quantum-safe solutions into their existing cyber security planning and life-cycle management, where they can be evaluated for functionality, performance, ease of use and other factors. Where necessary, existing infrastructure can be enhanced or replaced. And all this can happen before these changes become critical to the security of the organization.

Organizations must also be able to protect their sensitive information throughout its entire lifetime. Information considered to be safely stored or transmitted because it is encrypted, could become vulnerable to a quantum computer during its lifetime. Understanding this risk requires examining current cyber defences and potential threat actors' access to quantum computing technology.

Managing the transition of the full array of tools used to protect a breadth of business functions and information assets may seem like a daunting task with no clear starting point or priorities. A Quantum Risk Assessment is an ideal approach for identifying and prioritizing the threats and vulnerabilities and laying the groundwork for reliably and cost-effectively evolving your systems to be resilient to quantum attacks.

QUANTUM RISK ASSESSMENT METHODOLOGY

A quantum risk assessment furnishes an organization with the knowledge they need to understand the extent of their quantum cyber risk, and the timeframe in which quantum-enabled threats are likely to emerge. It will provide a basis for an organization to address quantum risk proactively, to build a roadmap to a quantum safe state, and to implement and validate quantum safe solutions as part of normal life cycle management rather than as a response to a crisis.

A quantum risk assessment (QRA) does not replace a normal cyber risk assessment (RA). Some of the information gathered during an RA is also required by the quantum process, so the QRA is generally conducted in conjunction with or subsequent to a traditional RA. However, the QRA is focussed on the specific security issues that emerge with quantum computers; it does not directly address several aspects found in a traditional assessment process.

Several years ago, Dr. Mosca proposed a model for evaluating quantum risk[2]. The six phase QRA process described here is consistent with risk assessment models from organizations such as NIST, and also incorporates Mosca's "x, y, z" quantum risk model.

Phase 1

> Identify and document information assets, and their current cryptographic protection.

As with any risk assessment the QRA begins with an inventory of important assets. The focus here is on sensitive or valuable information assets which require cryptographic protection, in accordance with the organization's security policy. It is important to identify the nature of the cryptography being used, how encryption keys are generated, stored and applied, and the origin of tools or appliances employed in these processes.

At a high level, an organization must understand the nature of its sensitive / valuable information, including its business value, access control and data sharing arrangements, backup and recovery procedures, and how it is handled at end-of-life. Many organizations have legal or regulatory requirements that influence these. A comprehensive review of all these factors are required to determine the organization's vulnerability to external and internal threats.

Phase 2

> Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.

This phase is not unique to a specific QRA, rather it is a continuous process conducted by a team of quantum technology experts who understand the obstacles and developments being encountered in several fields of quantum research, and can use the information to forecast the likely timeline for delivery of a quantum computer and to understand its impact on an organization's cyber security.

There are many sources of information on the state of quantum technology, but understanding the relevance and true impact of specific research developments is not a trivial process. Having either a dedicated team of quantum experts or a relationship with an organization specializing in quantum technology is critically important to completing a QRA. There are multiple groups around the world conducting independent research and using various approaches to develop quantum computers and quantum-safe cryptography. It is critical to have access to experts who follow developments in both fields, and can contextualize them to forecast their cybersecurity impact.

Ideally, findings from this phase of the QRA are used to influence the development of quantum-safe cryptography. Working with quantum experts having strong connections to academic and research communities permits real-world problems uncovered by the QRA to influence the direction of quantum-safe research.

[2] M. Mosca, "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop", e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26-27 September 2013

Phase 3

> Identify threat actors, and estimate their time to access quantum technology "z".

A security conscious organization will be aware of their most significant threat actors, and will have a list of previous attempts to penetrate their cyber defences. A QRA considers the impact of quantum computing on these threats, focussing on the likelihood that they will be able to exploit quantum computers and the timeline for their access to them. We will also consider new threat actors who might emerge once quantum computing becomes a reality. Taken together, these form the Collapse Time (z) portion of the Mosca model, which is the time until current cyber defences collapse in the face of threat actors with access to quantum technology.

This process again requires continuous evaluation by experts with knowledge of developments in cybersecurity and quantum computing.

Phase 4

> Identify the lifetime of your assets "x", and the time required to transform the organization's technical infrastructure to a quantum-safe state "y".

Determining the useful lifetime of your business information is critical to understanding your organization's quantum vulnerability. If an adversary can capture and archive your encrypted information, how long will it remain useful? This will be governed by the nature of your business, your products and your clients, as well as by regulatory requirements that may apply to your organization.

We consider the tools available to combat a quantum-powered threat actor. How effective are current policy and procedures at protecting the organization's encrypted information from both internal and external threats? We examine the strength of the existing cryptography, and how effectively it is being applied and used. We review available quantum-safe cryptographic methods, to determine whether they might be appropriate replacements for existing capabilities. We may reach out to the vendors who have produced the products in use by the organization, to identify whether new algorithms or protocols could be implemented within existing tools and appliances or whether upgraded equipment may be required. Reviewing the policies, management and procurement processes that apply to your organization's IT and security infrastructure, we evaluate whether quantum safety can be integrated into the organization's IT lifecycle management processes.

Having this information we can compute the remaining values of the Mosca model- the Shelf Life of an organization's data (x) and the infrastructure Migration Time (y).

Phase 5

> Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. (x + y > z ?)

Using the information gathered to this point, we are able to assess the risk the organization faces as quantum computers emerge. The lifetime of sensitive data is considered, including its likelihood of exposure; and combine that information with the time required to migrate existing processes and infrastructure. This is compared to the timeframe in which quantum technology will be available to relevant threat actors. Taken together, this provides a reasonable estimate of when the organization needs to be taking active steps to mitigate quantum risk. It is possible that some organizations may already be facing this risk, depending on the lifetime of their data and the processes in place to protect it today.

Next we will want to assess the business process impact

that results from the changes we anticipate. How long will it take to implement the necessary changes in products, protocols and procedures? Will quantum-safe technologies introduce latencies, reliability or performance issues that need to be addressed? Are there policy or procedural changes required to improve the revised system, or the overall security of the organization's information?

Phase 6

> Identify and prioritize the activities required to maintain awareness, and to migrate the organization's technology to a quantum-safe state.

The quantum risk assessment provides information and guidance towards a quantum-safe status, but it is unlikely this state can be achieved with the tools and technologies available today. Quantum technologies continue to evolve, as do our understanding of the strengths and vulnerabilities of quantum-safe approaches. Migration plans also need to respond to changes as vendors incorporate these developments into their products and tools. It is important to track all these, and most organizations should develop a roadmap that addresses immediate concerns while permitting the incorporation of new quantum technologies as they become available.

Any cyber risk assessment must be periodically updated to account for emerging threats and to take advantage of improved security solutions. This is particularly true for quantum technologies, which are rapidly evolving. Multiple quantum technology options are being explored at this time but not all of these pose the same cyber security threat, and it can be difficult to assess the impact of any specific new quantum development. Thus it is recommended that a QRA be the first step in building a roadmap to quantum safety.

This roadmap will be designed to ensure continued access to specialists who follow these technologies and understand the implications of new developments in quantum computing and quantum cryptography. It can provide a basis for opening discussions with an organization's employees, partners, customers and product vendors, ensuring that all are aware of the steps being taken and ensuring they understand the impact this will have on their own processes and infrastructure.

WHAT DO I DO RIGHT NOW?

If your organization uses the Internet for any important business process, then cryptography is almost certainly employed for cyber security. Therefore, you cannot afford to wait for the emergence of quantum computers to understand the risks you face.

Take steps to:

- *Ensure you have a current, thorough organizational inventory which includes details of embedded cryptography that may exist in a variety of products;*
- *Monitor your environment for threats, and ensure that you conduct regular risk assessments;*
- *Conduct a quantum risk assessment as part of or subsequent to the regular risk assessment process;*
- *Understand your telecommunications and security vendors' posture on quantum computing, which of their products will be affected and their preparations to manage this risk;*
- *Evaluate quantum readiness as part of your current procurement processes for network and security systems; and ask your current vendors to discuss the state of their quantum planning;*
- *Work with an informed partner to track developments in quantum computing and quantum safe solutions, and to establish a roadmap to quantum readiness for your organization.*

The most important message is to Act Now! The organizations that are most at risk are those who wait for quantum computers to arrive or to avoid action until perfect cryptographic solutions are developed. This is almost certainly guaranteed to have your organization scrambling to deal with their sudden vulnerability to quantum attack in the foreseeable future.

About the Authors

Dr. Michele Mosca
Co-founder and CEO, evolutionQ Inc.
Co-founder, Institute for Quantum Computing, University of Waterloo, Canada

Michele is an award-winning researcher whose cutting-edge work on quantum computing has been published widely in top journals and textbooks. He is globally recognized for his drive to help academia, industry and government prepare our cyber systems to be safe in an era with quantum computers. He is co-founder of the Institute for Quantum Computing (University of Waterloo) and a founding member of the Perimeter Institute for Theoretical Physics. He co-founded evolutionQ Inc. to help organizations evolve their quantum-vulnerable systems and practices to quantum-safe ones.

John Mulholland
Director, Quantum Risk Management, evolutionQ Inc.

John leads the development of quantum threat and risk assessment processes for evolutionQ Inc. Having established a framework for quantum assessment, he works with a team of globally renowned experts in quantum science, technology and cryptography to help organizations understand and manage the cyber security issues emerging with quantum computers. John has worked with organizations in government and industry to assist the migration of their systems and practices to quantum-safety.