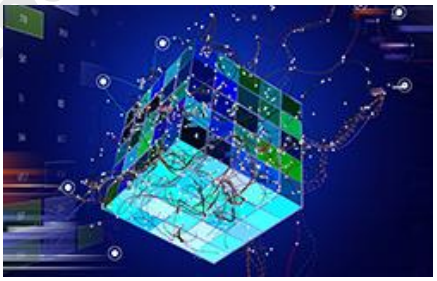
www.pipelinepub.com
Volume 22, Issue 1

Why Security Agility and Resilience Are Critical in the Quantum Era

By: Martin Charbonneau



Communications service providers (CSPs) have played a leading role in digital transformation for decades. They have shepherded enterprises through massive technological shifts, from enabling global connectivity to delivering services in the cloud. Now, the paradigm is shifting again, driven by the looming threat of quantum computing that will present entirely new challenges for cybersecurity.

The risks posed by quantum attacks are likely to affect every industry, making quantum defense an immediate national and economic imperative. As the backbone of today's digital communications, CSPs are ideally positioned to lead that defense. They already play a critical role in protecting sensitive data for governments, banks and enterprises, operating infrastructure at scale and across borders. By enabling a defense-in-depth approach, they'll be able to extend this expertise into the Quantum Era—and deliver the agility and resilience needed to maintain trust in the networks that connect the world.

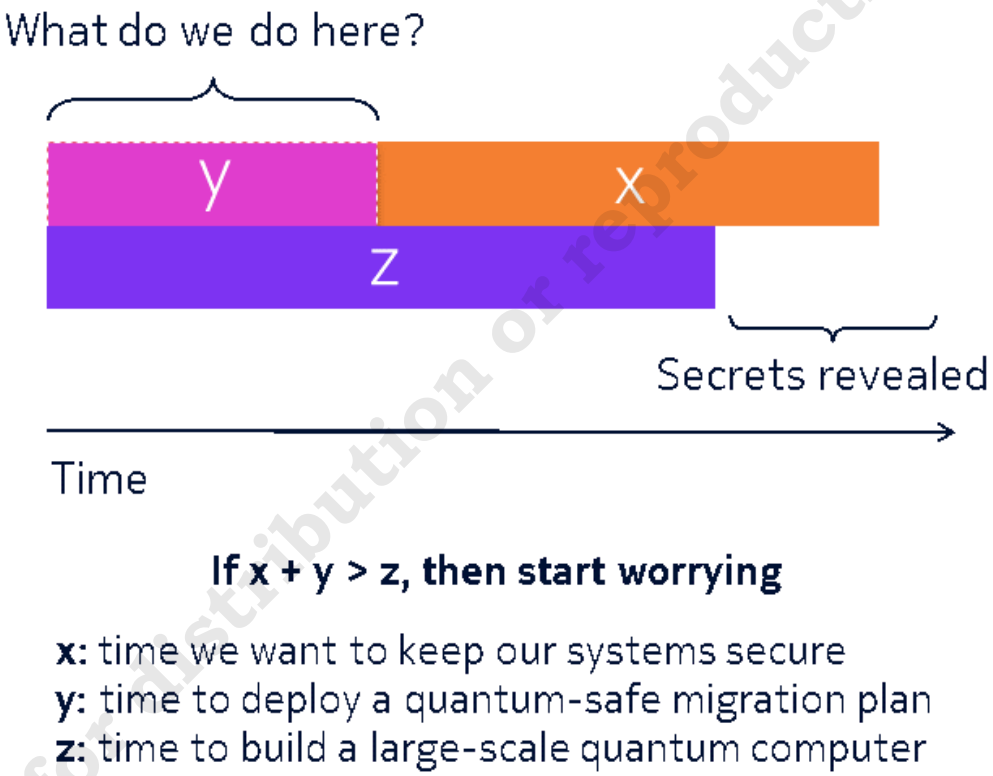
The Urgency to Act

Quantum computers can perform tasks exponentially faster than traditional binary computers. They can also carry out multiple processes at once, further increasing their capacity and speed. The potential benefits to society are numerous. However, if they fall into the wrong hands, quantum computers could be used to break most of the encryption methods currently used to protect financial transactions, personal data, intellectual property and other sensitive communications. Although quantum computers that can do this don't exist yet, they are coming soon—possibly within the next five to 10 years—and the moment of their arrival is known as Q-Day.

But data are already at risk, particularly from a cyberattack strategy called 'harvest now, decrypt later.' Cybercriminals are likely already exploiting existing weaknesses and harvesting massive amounts of encrypted data, even if they can't do anything with the data at the moment, knowing they can just hold onto it until quantum capabilities advance enough to decrypt it. In other words, organizations can't afford to wait for Q-Day before they worry about protecting themselves.

To illustrate, consider Mosca's Theorem, as shown in Figure 1: If X + Y > Z, a business is at risk. **X** is how long the company has to hold its data securely. For data that becomes irrelevant as soon as it is used, that number might be close to zero, while other types of data need to be held onto for years. **Y** is the time it will take the business to deploy quantum-safe cryptography and apply it to all its applications, which can take significant time. Finally, **Z** is the time until Q-Day—and that number is not static. In fact, it gets smaller every day.

For some organizations, X + Y may not be considerably longer than Z. But consider sectors like healthcare, finance and government. These sectors are often legally required to keep data secure for decades. If they're not already using quantum-safe cryptography, their data may have already been vulnerable for some time. That means they absolutely must act *now*.



Governments around the world are also recognizing the quantum threat and have begun enacting laws, standards and regulations for quantum security. In the United States, the National Institute of Standards and Technology (NIST) has identified an initial set of standard post-quantum cryptographic algorithms, which governments around the world—including those of Canada, Japan and Australia—have begun incorporating into their own cybersecurity strategies and standards.To address the quantum threat and meet impending compliance deadlines, organizations must begin planning their migrations now. Fortunately, CSPs are ideally positioned to help.

From Basic Protection to Defense in Depth

Just as end users implicitly trust a given business to protect the data they provide and the applications they use to interact with it, the business, in turn, trusts CSPs to deliver a secure networking environment. However, in the Quantum Era, the expectation of security will start to shift. The advent of quantum computing, combined with the power of artificial intelligence (AI), makes it increasingly unrealistic for any organization to expect to never experience a breach. It must be assumed that even post-quantum cryptography will ultimately be broken.

As the Quantum Era approaches, businesses must evolve their approach to organizational risk mitigation, placing network security at the heart of their strategy. The best defense against the coming threat will be a defense-in-depth strategy that incorporates multiple types of protections: symmetric cryptography at the optical, IP and MPLS layers of the network, as well as public key encryption with post-quantum cryptography at the application layer.

At the network layer, cryptographic technologies can be embedded directly into a CSP's connectivity solutions, including symmetric encryption like AES. These can be complemented by a symmetric key distribution infrastructure, which can take various forms, including quantum key distribution. This type of infrastructure will help protect the network from the bottom up while also supporting the use of dual-use technologies across both civilian and defense domains.

This defense-in-depth strategy enables both cyber-agility and cyber-resilience, two critical capabilities in an era in which preventing every cyberattack is no longer a realistic goal.

Cyber-agility refers to the ability to adapt quickly, such as switching post-quantum algorithms when they become vulnerable or compromised. This flexibility allows organizations to pivot rapidly if a particular encryption method is broken.

Cyber-resilience involves deploying multiple layers of protection through complementary key distribution infrastructures. It empowers organizations to respond to, contain and recover from security incidents more effectively, helping maintain operational continuity.

CSPs have an advantage in securing the network, thanks to the fact that they operate their infrastructure at scale and can therefore deploy consistent quantum-safe protections across diverse customer environments. Network-level safeguards are also faster to deploy than application-layer protections and can provide a resilient buffer to protect customers that haven't yet migrated or re-certified their applications for post-quantum cryptography. This matters because comprehensive protection requires coordinated efforts across both the network and application layers.

The Business Case for Quantum Security

Despite its benefits, some CSPs who look at quantum-safe protection as just another new network feature might find it hard to justify the costs, primarily because it can seem difficult to immediately monetize. That's because quantum-safe networking is more like the locks and security cameras a store owner might install on their premises. These things do not generate revenue, but they protect the business and its assets. In other words, they're a cost control or risk-mitigation measure. Thinking about quantum-safe networking in those terms makes its value much clearer.

But that doesn't mean there's no way to derive added value from quantum-safe services. CSPs can offer premium tiers of security as part of their service packages or provide advisory or managed services to help customers transition to quantum-safe outcomes, like quantum-safe data center interconnections or quantum-safe cloud access. To make the offer more appealing, it can even be tailored to each customer. For example, some will be happy to let the CSP manage key generation and distribution, while others will prefer to take a more hands-on approach. CSPs that can offer both options will be better positioned to derive more value from their quantum-safe offerings.

The Quantum Imperative Starts Now

Quantum threats are no longer distant, far-fetched possibilities. They're coming sooner than one might think—and a lot of data are already vulnerable. That means quantum security is no longer an optional feature.

Nevertheless, achieving that is not as costly or onerous as some CSPs might expect. It's usually a matter of upgrading their existing devices and components to incorporate the latest cryptography methods, rather than a massive lift-and-shift or re-engineering of the whole network. In most cases, these upgrades can be accomplished fairly quickly at relatively little cost.

The alternative—waiting for something bad to happen and then dealing with the fallout—is what is truly costly. CSPs that take the initiative now, protecting their own networks and supporting their customers through their quantum-safe transitions, will become leaders in the Quantum Era—shaping the security narrative for the next decade, gaining a competitive advantage and strengthening their long-term relationships.