Insights from IBM Think Circles

Quantum computing in supply chain

Preparing for near-term threat management and planning for longer-term operational advantage

"Make no mistake. The impact is coming—and it's not a question of if, but how soon and how disruptive."

The near-term threat

Experts predict that commercial applications of quantum computing will proliferate when quantum computers achieve a level of power, predictability, and stability that is likely in the next decade. But even today, threats are looming.

Remember Y2K, the infamous computer bug that threatened to bring down the world's computer systems as we entered the new millennium? Well, get ready for Y2Q—the point when bad actors using quantum computers will be able to destroy known encryptions, exposing every bit of data that's ever been collected. These risk scenarios are likely much sooner than business advantage because stability and predictability don't matter to cyber terrorists—a quantum encryption hack just needs to work once for data to be exposed.

Have we got your attention? The latest in a long line of disruptions and threats to supply chains—and all business operations—is imminent, yet only 12% of supply chain executives predict that quantum computing capability will be incorporated into supply chain operations by 2025.[1]

Members of IBM's elite CSCO Think Circle voiced their thoughts, fears and plans—and we're sharing their insights so we can make Y2Q as much of a non-event as Y2K.

Quantum computing in a nutshell

Quantum computing is a powerful technology that will exponentially increase compute power, improving the way we analyze data. Based on the principles of quantum mechanics (ask your favorite chat bot to define quantum entanglement, superposition, and teleportation for more detail), engineers have been perfecting quantum computing capabilities for decades. We're now seeing unprecedented growth in its development. In just three years, we've gone from 24 qubits to over 400, with expectations that we'll reach 1,000+ by 2024.

"I'm not sure how, but we have to take the entanglement and teleportation of Quantum computing to a practical level."

However, that compute power comes with a downside. There is an increased risk of security threats from bad actors who could use quantum approaches like Variable Quantum Based Factoring to invade and overpower our current data encryption methods. This could lead to the most critical data and systems being compromised, such as those that run governments and businesses—airlines and banks, for example—and could severely compromise all of our personal data and identity transactions.

"All organizations are being forced to be in the business of transparency and visibility to the consumer. How do I provide that transparency and protect the vulnerabilities at the same time?"

Vulnerabilities increase significantly as we move from the cloud to distributed applications and edge technologies. This is further amplified by the undocumented and unknown, rogue or non-compliant tools, processes and workflows that proliferate unnoticed in many organizations. There are two types of threats: 1) access to current encrypted transactions and "crown jewel" business critical information and 2) already harvested files that bad actors are poised to access when they can. Although it's hard to define when Y2Q will arrive, the Thinkers believe it's somewhere between 3-7 years away, which, for purposes of planning and preparation is... NOW.

While there's a terrifying potential of Y2Q, some organizations are already experimenting with quantum to test modeling and optimization, which can lead to greater opportunities for efficiency, productivity, resilience, and agility. In essence, despite the threats, supply chain Thinkers are optimistic that quantum can help them find new ways of solving old problems. The Thinkers also noted that in addressing risk mitigating/threat analysis there would be added business benefits of rationalized workflows, applications and business control.

The longer-term business opportunity

Supply chain Thinkers agreed that perhaps the greatest near-term opportunity to use quantum computing in supply chain operations is modeling. The benefit of better managing the sheer complexity of these models is enormous. Imagine optimizing transportation and logistics, simplifying the variability of planning, safely sharing protected data through a convoluted network of ecosystem partners, and for capturing all the value of digital twin simulations.

"I think we're getting a good understanding of how complex the model is in supply chain, with the multiple variables. Trying to get to automation of a model with infinite variables is impossible. The opportunity for quantum is to simplify the model."

The game changer just might be the marriage of quantum computing and edge computing. The amount of raw data that sensors can collect is now impossible to analyze in real-time with today's classical compute capabilities. But it's possible with quantum.

To best plan for the kind of infrastructure that will be needed, Thinkers highlighted the "rubber band" challenge: the operations technology pull to the Edge and the information technology pull to the Cloud. CIOs are pushing ERPs and other strategic applications to the cloud as rapidly as possible to build the sacred "one version of the truth." Meanwhile supply chain operations execs are automating at the Edge for real-time machine learning and end-to-end visualization at the device level.

With quantum computing, the possibilities and innovations are endless, and perhaps the OT/IT "rubber band" will not need to stretch so thin.

"If you could get a quantum computer at the Edge that could analyze data in real time, that would be game changing."

How to prepare for near-term threat management and plan for longer-term operational advantage

While none of the Thinkers believe their organizations are ready to fully address both the challenges and opportunities of Y2Q, they are game to do more. Here's where they suggest starting:

- *Make an explicit decision about building two teams to address quantum:* a threat team and an advantage team. Empower the threat team to take immediate action, while the strategic team should be positioned to take a longer-term approach to building quantum advantage. Include people from technology, security and operations, both within your organization and across your business ecosystem.
- *Threat team:* identify where data may already have been harvested. Use process mining and forensic modeling to understand possible vulnerabilities in your business workflows.
- *Advantage team:* run strategic garage sessions to innovate, ideate, and incubate longer-term opportunities that fundamentally challenge the business orthodoxies of the past and build new models for the future.

"You forced me to think about this more than I had been. I'm now going to force some next steps internally by talking with COO, CIO. I think I need to have a frank discussion about where are we now and where we need to be so we feel more comfortable."

"This conversation has opened up my mind on several topics. I'm (planning to) connect with CSO on security side and CIO. I'm not sure how much we are thinking about this from a vulnerability standpoint, but it needs to be on our radar if not top of mind."

"This has to be a network conversation—it can't be a single company conversation. Everything to do with quantum, we all have to move together or none of us can be secure."

Related IBV reports

Security in the quantum computing era
ibm.co/quantum-safe

The quantum decade is here
ibm.co/quantum-decade

Exploring quantum computing use cases for logistics
ibm.co/quantum-logistics

IBM Institute for Business Value
Published in partnership with IBM Think Circles

1 IBV Supply Chain Resilience Study, 2022