Why all CISOs need to prioritize quantum

Dekker, M.

Publication date
2022
Document Version
Final published version

Why All CISOs Need to Prioritize Quantum Tech Today

Martijn Dekker, Chief Information Security Officer, ABN AMRO

For most CISOs who think about quantum technologies at all, it is a vague consideration for a day far in the future. It is hard to prioritize it when we have so many concerns we need to deal with today. Investing resources in quantum technology now seems like a long game we simply cannot afford to play. However, while quantum computing may still be in early stages of development, there are several other quantum technologies already in use that are relevant for CISOs in financial services. We ignore them at our peril.

“Nobody Understands Quantum Mechanics”

So said the great physicist, Richard Feynman. If he said that about his quantum physicist colleagues, the rest of us have little hope, but here are the basics: quantum computing leverages two special properties of quantum mechanics: entanglement and superposition. This is different from classical computing, which uses electronics to encode data and logic into bits that can be either on or off. Quantum computing uses quantum states, or qubits, that can be on and off at the same time. The promise of quantum computing is that this weird behavior can be used to design algorithms that will outperform any classical computer that one could ever build.

Infinitely more powerful computers would transform our entire technology infrastructure, especially in financial services. For cybersecurity professionals, the rise of quantum computing will require a new vision of security that maximizes the advantages and minimizes the risks inherent in the adoption of quantum technology.

MARTIJN DEKKER

Dr. Martijn Dekker was appointed Chief Information Security Officer (CISO) of ABN AMRO in early 2014. In his role as CISO, Martijn is responsible for defining, overseeing and implementing the information security...

Read More

The Sky Might Not Be the Limit

Success in financial services is based on our aptitude for prediction, risk modelling, and optimization. For security teams, this includes functions like fraud and intrusion detection. All of these use algorithms based on linear algebra to crunch data and spit out answers. But because of the limitations of compute power, we must include assumptions in our models that limit their accuracy in order for the computer to actually be able to do the calculations. Quantum computing promises no such limits, which means more accurate models that arrive at answers exponentially faster than the most powerful classical computers in existence. What financial firm wouldn't want that?

Of course, quantum computers come with new risks, the most obvious one being their potential ability to break cryptography. It is not correct to say that information security people secure assets. What we actually do is put off access to assets for such a long time period that the data will no longer be relevant to potential threat actors, i.e. a million years. Current cryptography relies on the assumption that cracking the code is computationally difficult. But that assumption falls apart with quantum computers.

Beyond cryptography's use in standard information security, cryptocurrencies like bitcoin are (currently) built upon the premise of mining – using computing power to find the correct random numbers that solve a complex equation. Solving these puzzles is what adds new blocks of data to the ledger of bitcoin transactions (i.e. the blockchain). A large enough quantum computer could speed up mining exponentially and potentially break the cryptographic keys of bitcoin wallets. With digital assets becoming part of the mainstream financial ecosystem, security teams will need to understand how to protect them in a world where threat actors have access to quantum computers.

You Snooze, You Lose

The big question, and the reason many delay dipping their toe in the quantum bucket, is when will quantum happen. Many consider it to be ten years away, and people have been saying that for 20 years. Why is it taking so long? Because building a powerful, reliable, general purpose quantum computer turns out to be an incredibly difficult engineering problem.

However, that does not mean you have ten years not to prioritize quantum technologies. On the contrary, CISOs must start familiarizing themselves with quantum tech now for the following reasons:

1. Major technological shifts do not happen in a linear fashion. They operate on exponential curves, meaning they start off slow, but then gain momentum and make huge leaps very quickly. One point on the curve before ten years is five years, meaning that even a relatively small breakthrough could dramatically accelerate the timeline.

2. The drivers to advance quantum technologies are increasing in force. The big tech firms and academia are investing huge sums of capital into quantum. There are also geopolitical motivations, especially the rivalry between China and the United States, who both have multiple national security use cases for quantum tech. Its development may be significantly

further along than is known in the public domain.

3. It takes a decade to replace cryptographic standards. Consider the SHA1 (Secure Hash Algorithm 1), whose weaknesses were discovered in 2005. It was only in 2017 that it was retired from use in popular browsers. If we assume quantum computing is ten years away, we should begin looking for quantum safe cryptographic replacements now.

4. Quantum tech is already here. Having a general purpose quantum computer may be the end game, but several other quantum technologies relevant to fincyber professionals are actually in use today.

- *Quantum communication* is a tamperproof way of transferring data – which is the holy grail of information security. It leverages quantum entanglement and superposition to build a secure communication channel between two parties with secret keys, where you can know if someone else is "listening in" to the conversation. This is not science fiction. China has established quantum communications links over thousands of kilometers via satellites and crystals in space. Several universities in Europe are also doing it via glass fiber. People are building a quantum backbone for a secure internet as we speak, which is obviously something any CISO must pay attention to.
- *Quantum sensing* is an alternative to GPS. Based on one starting point, a machine can consistently calculate incredibly accurate space and time measures. One prime use case for this is warfare. The US Department of defense is investing in quantum sensing because both troop movements and weaponry are dependent on GPS, which is vulnerable to jamming by enemies. On the flip side, GPS is controlled by the US government, who could conceivably turn it off at any time. Countries such as China are interested in autonomous networks for geopolitical reasons, but many industries, such as telecoms, currently depend on GPS for accurate time measurement. In finance, trading requires time measurements down to the nanosecond and beyond. Quantum sensing could also be used for internet of things (IoT), mobile banking, and more.
- *Quantum randomness*: What we think of as random generators, which we use for everything from passwords to hashes to keys - are actually only pseudo-random. We already know that hackers can use the bias in current generators to predict the next "random" number. But quantum tech can generate truly random numbers.

Get Ahead of the Quantum Curve

Here is how CISOs can start preparing for the quantum age now:

1. Familiarize yourself with the spectrum of quantum technologies now in use, and by the time quantum computing is real, you will not be taken by surprise.

2. Leverage quantum in your own security measures. Prioritize crypto agility and include quantum from now on in all lifecycle management decisions and procurement procedures. Many software providers are already

doing it – so you may be implementing quantum-safe solutions without even knowing it. This will become even more urgent as digital assets and cryptocurrencies, which rest on the premise of secure cryptography, gain wide adoption across financial services.

3. Learn how to protect quantum technology, because your business will use it and you will be asked to secure it. Consider questions like how to ensure integrity of quantum assets.

4. Get access to quantum talent If you cannot hire quantum expertise directly, partner with universities or tech companies to make sure your technology and security infrastructure keep up with quantum advances.

As always, your adversaries will use the tech sooner than your business. Also be realistic: quantum technology will be part of every CISO's roadmap; this holds for many technologies. So quantum technology should not be your only strategy.

We have seen over and over that technological development is itself a stronger driver than the economic, political, and social implications of the technology. If we can develop it, we will, simply because it is possible. Quantum brings with it the potential for a wholesale change in how we do business, but for now, that change is slow. That gives us time to think strategically about its implications and plan accordingly. But that time will be up before we know it. We must act now.

The Insight

Just because the arrival of general purpose quantum computing is still several years away, CISOs ignore quantum technologies at their peril. Several relevant quantum technologies, such as communications, sensing, and random generators, are already in use. CISOs should familiarize themselves with current quantum tech, start including quantum safe solutions in their lifecycle management, focus on improving crypto agility, and prepare for the implications of infinitely more powerful computers today.

March 2022