BRIT

writing the future

will quantum computing break encryption?

Quantum computing is changing the way we think about encryption and security

In the past, the concept of quantum computing was largely theoretical. Computing scientists have theorised about the idea of quantum mechanics being applied to computing since the eighties. However, in 2022, we are edging closer to the sometimes mind-boggling world of quantum computing becoming a reality.

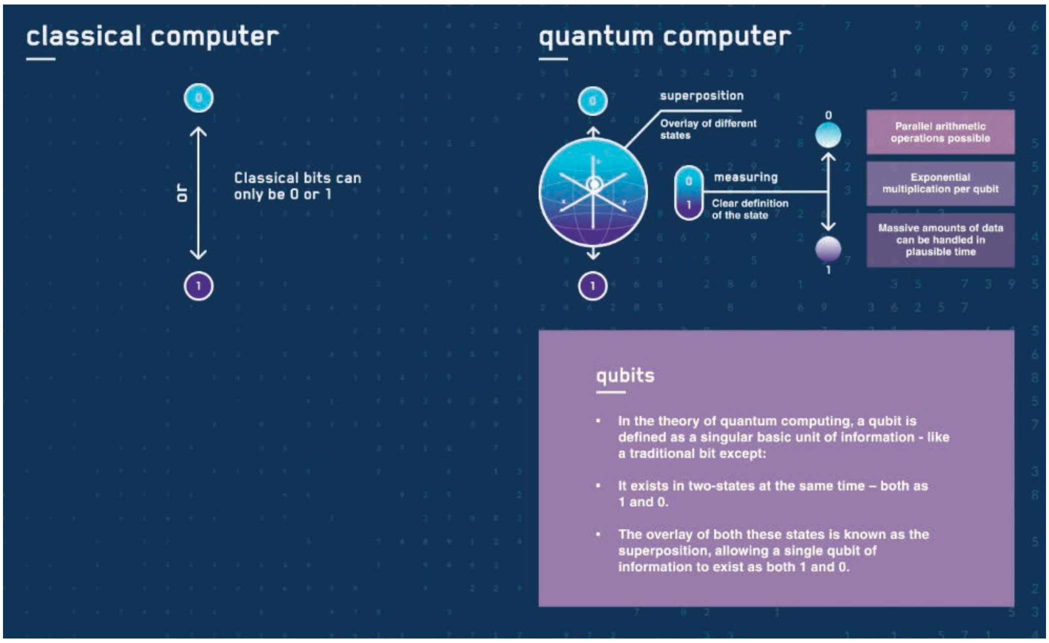
In light of quantum computing developments by various tech giants and quantum start-ups, even conservative estimates have imagined this innovation being commonplace as early as 2035. Consequently, Information Security or 'Info Sec' professionals need to understand the implications of the proliferation of quantum computing and what it means for encryption and security.

What do we mean by quantum computing?

Before we delve into the specifics of how quantum computing will change the way we approach cyber security, let's start with some basic concepts. The theoretical side of quantum computing has been discussed for around 40 years. Here's a basic definition to get us started;

Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory (which explains the behaviour of energy and material on the atomic and subatomic levels). Computers used today can only encode information in bits that take the value of 1 or 0—restricting their ability.

Quantum computing, on the other hand, uses quantum bits or qubits. It harnesses the unique ability of subatomic particles that allows them to exist in more than one state (i.e., a 1 and a 0 at the same time).


classical computer
0
or
1
Classical bits can only be 0 or 1
quantum computer
0
superposition
Overlay of different states
1
0
1
measuring
Clear definition of the state
0
1
Parallel arithmetic operations possible
Exponential multiplication per qubit
Massive amounts of data can be handled in plausible time

qubits

- In the theory of quantum computing, a qubit is defined as a singular basic unit of information - like a traditional bit except:
- It exists in two-states at the same time – both as 1 and 0.
- The overlay of both these states is known as the superposition, allowing a single qubit of information to exist as both 1 and 0.

continued

Quantum computing is a complex subject that many of us won't encounter in our day-to-day lives, but the main takeaway is that the technical possibilities are enormous. Several applications are beginning to be fully realised across a number of different industries;

Healthcare

Quantum computing can be used in drug development, simulating interactions between experimental drugs and the fully mapped human genome.

Meteorology

Quantum computers could be used to predict weather more accurately through pattern recognition and generating more detailed climate models.

Finance

Algorithmic trading could be developed with quantum computers to automatically trigger share dealings based upon a variety of market variables at scale.

Technology companies including Google, Microsoft and IBM are all working to bring quantum computing to the mass market across a variety research projects. Just last year, a major step forward was secured as British firm Orca claimed to have used photonics to make the adoption of quantum computers more commercially viable. As the reality of quantum computers is now a question of "when", rather than "if", we need to think about the knock-on effect this will have for computer security.

How will traditional systems be threatened?

InfoSec specialists have traditionally created security systems and protocols to protect from the threat posed by existing computer hacking systems. When looking at quantum systems and their potential for nefarious activity, a few points should raise alarm bells.

Firstly, as quantum computers are complex systems, they will likely be accessed via the cloud remotely. This creates low barriers to access that may be easy for hackers to exploit.

Additionally, as quantum theory sets to increase the capabilities of computers, the points of vulnerability within current security measures will also increase. It's thought that in a matter of seconds, quantum computers will be able to solve problems that would take traditional computer years. Cyber tech specialists are coming to the realisation that even the most advanced security systems in place today could be easily toppled by a quantum computer.

Managing the future risk

It's the duty of infosec professionals to manage the future risk that the development of quantum computer systems might present. Expert insight from the Wall Street Journal included a number of steps that can be implemented and considered alongside the roll-out of quantum computer systems;

- Build Awareness of the risks of quantum to security
- Prepare cryptographic systems for the quantum era
- Become more agile to the developing threat from quantum computers
- Practice good cyber hygiene

Creating these new future-proof protocols is known within the industry as post-quantum cryptography or PQC. These protocols will spread awareness of the problem that needs addressing but are by no means a silver bullet to solving what issues might come over the horizon.

continued

The challenge ahead

While PQC is one of the best precautions we can take for the world of quantum computing vulnerabilities, there is a two-fold problem with implementing the necessary protection.

Firstly, there is a high cost associated with updating to a new security standard. Upgrading legacy systems can be costly for businesses. This is often down to the incompatibility of existing protocols, the inadequacy of a company's inventory of all the vulnerable nodes in their IT system that require upgrading (made even more difficult when third party vendors are involved), along with efforts to make these changes over longer periods to help manage costs. This is exacerbated further when we consider any possible resistance from management, who might question the need to trade out existing security systems for a risk that isn't fully realised yet.

The second challenge is the question of data interception where data has been stolen, but not decrypted. The concept of a "harvest today, decrypt tomorrow" hack has given cause for concern for infosec professionals as information that has previously been compromised might risk decryption from a quantum computing system in the future. Paolo Cuomo, our Director of Operations, believes this to be an issue for the security specialist of today, not a few years down the line when quantum computers become more prevalent.

In a recent piece for LinkedIn, Paolo shared his thoughts:

"What if fully-encrypted data was stolen and held onto? As long as the data expiry period is longer than the period before decryption is possible, there is value to the thief and damage to the original owner.

Furthermore, when a hack becomes public, changes are made to stop the problem. If data is being stolen and no noise made about it, how long might the security hole remain open allowing a continual syphoning off of that data?

This concept of harvesting data today and then decrypting it in the future is what makes this top one of real urgency. Urgent for information security teams to think about; and urgent for cyber underwriters to consider."

Paolo Cuomo
Director of Operations

Paolo states that the decade or so we have before the power of quantum computing is fully realised, might not be enough time, asking, "how long does it actually take to replace encryption protocols built into hugely complex IT and communications systems?" We can't know for sure if famous security breaches for brands like MySpace, the Marriott, or MyFitnessPal could rear their heads again if quantum computing solutions can decrypt the stolen data. But we made be behind in the race for protection.

So, even though cyber security professionals may feel too busy to consider longer-term risks, the threat posed by quantum computing is not something they can completely ignore. At the very minimum, infosec professionals should:

- Include quantum computing in their risk assessment and develop a roadmap for managing this risk.
- Identify whether quantum computing is being investigated elsewhere in the business (for positive purposes) to use that expertise.
- Define the route to cryptographic agility within their organisations to ensure a swift transition to PQC protocols once they are standardised and available.
- Factor in that encrypted data today is not guaranteed to remain safe in the case of a breach.

How Brit are preparing

There is a lot to think about a prepare for over the next decade as quantum computing systems become more prevalent in our daily lives. We are preparing our clients to respond to the evolving risk landscape through our knowledge of this technological innovation.

Get in touch with our Cyber team to be more proactive about managing your clients' full range of cyber risks.