Picture credit: AdobeStock

# IMPENDING THREAT

**Nils Gerhardt** *considers post-quantum cryptography in the boardroom*

**The most up-to-date developments in quantum computing are often in secret and any information that makes it to the public should be treated with caution**

**Nils Gerhardt** has 19 years' experience in the cyber security industry. In his current role, Nils is the Chief Technology Officer and head of product for Utimaco, and supervisory board member of ISITS AG.

**The idea of a quantum computer is now 44 years old while the average C-suite executive is aged 57. While Paul Benioff was describing a quantum-mechanical model of Turing machines (put simply, how computers could be made from extremely small objects) when he came up with the theory, the average decision-maker at a major company would have been 13, and the only place they would have heard the world 'quantum' would have been in comic books.**

Today, we would hope that there would be no top-level executives who haven't heard of quantum computing, especially when 100 percent of Fortune 500 companies and the majority of Global 2000 companies have a Chief Information Security Officer (CISO). However, securing themselves against quantum computing threats, which could arrive at any time, is something that will take engagement from an entire company. For companies working in certain industries, it could be a costly, lengthy process that involves securing millions of digital assets.

So, what does the rest of the boardroom need to know about Quantum Computing? Given that this is a new technology there is a huge amount of speculation and downright disinformation circulating that has a similar tone to other speculative bubbles in the tech industry (NFTs are the future, AI will replace our jobs etc.) The C-Suite has a lot on their plates already, so what information do they really need?

While the inner-workings of quantum computers are difficult to describe without going into the complex, counter-intuitive theory behind them, what most people need to know is that they could be hypothetically vastly more powerful than conventional computers.

To over simplify the complex world of digital security, a company's digital assets are protected by mathematics. The long and complex numbers that function as 'keys' to a particular digital lock could take upwards of trillions of years for a standard computer to solve, but they can be solved, and this means that the only thing preventing your digital assets being open to all is computing power.

'Quantum Supremacy', the point at which a quantum computer can carry out calculations for certain problems faster than a conventional computer, was achieved several years ago. While we are perhaps years or even decades away from a Quantum General Computer, the fact that they could break standard forms of encryption that all digital security relies upon has been known about for years.

The first and most significant thing to know about quantum computing is we don't know when commercially available quantum computers will be created.

Just as at the quantum level everything is a jumble of shifting probabilities and contradictions, the world of emerging quantum computers is similarly opaque. The systems themselves are being developed by governments and very large corporations such as IBM and Google, so the most up-to-date developments are often in secret, and any information that makes it to the public should be treated with caution.

Secondly, announcements that a company or government has achieved a new fastest quantum computer do not necessarily mean that we are much closer to working quantum computers. In previous races to deploy new technologies, like the Space Race of the mid-20th century, it was easy to see how a more powerful rocket would help one side get into space quicker, but with quantum computing the issue of error-correction makes advancements very difficult to quantify. Current quantum computers make one error in every hundred operations, but to be truly useful they would need an error ratio of one in a trillion. Algorithms can be used to compensate for these errors to a point, but to truly correct for them major advances need to be made in the systems themselves, and the problem is so severe that IBM has a ten-year roadmap for developing fault-resistant quantum computers. That in no way means that usable, fault tolerant quantum computers are guaranteed to arrive in 2034, but does mean that we need to question anyone who claims that it will arrive within the next few years.

While we wouldn't encourage any company to delay carrying out at the very least and audit of which of their resources need to be secure, there are industries in which deploying post-quantum cryptography should be a matter of absolute urgency:

## CURRENT QUANTUM COMPUTERS MAKE ONE ERROR IN EVERY HUNDRED OPERATIONS

- Companies selling goods with long lifecycles: the average car spends 11 years on the road before being scrapped, and a lot can happen in that time. As a rule of thumb, if a connected device is likely, or even possibly, going to be used for five years or more then you should make sure that it is prepared for quantum cryptography.
- Component manufacturers: For a similar reason, companies that manufacture components used by other companies also need to look at their quantum security. You won't know how long your components will be in use for, and their end-users may not know or be able to control the way they are secured, so it is best to be safe and protect them now.
- Critical infrastructure: It is likely that the first instances of harm caused by quantum computing are going to be between state actors, as opposed to smaller cyber crime gangs. In this case, critical infrastructure such as power, water and transport will be the first civilian networks to be targeted – this has been the case for literally decades and will only become more dangerous as states have access to quantum computing.
- Defence: It goes without saying that companies that either work directly with or around the defence industry, not just in their own country but in any, will be prime targets for state-based or aligned bad actors with access to quantum computing.
- Regulated businesses: Financial services and healthcare companies keep long-term (sometimes even cradle to the grave), highly sensitive data on their customers, and if this data is altered – or even could be altered – then this would have major effects on the world's financial environment, which relies on accurate records.

None of the above means that companies that aren't in these sectors are safe – if any company leaves itself unprotected then various bad actors will, in time, find a way to exploit that, perhaps by decrypting the data much later.

Although there is a great deal of complexity around quantum computing, organisations like NIST have already worked out quantum-safe algorithms to protect data, and hundreds or thousands of companies are already using them to secure their data, even though the threats to that data haven't emerged. Although we don't know exactly when quantum computing will go from being a hypothetical to a threat, it's important that the C-Suites of any and every company, not just the CISO, start preparing now by assessing what cryptographic assets are in use today that need to be protected against tomorrow's threats ●