Quantum in cyber risk is real – inaction is no longer an option

by **Alexey Bocharnikov**
EY Asia-Pacific Quantum Technology Leader

7 minute read
28 Jul. 2023

Related topics
Cybersecurity

The development of quantum computing has made it imperative for organizations to discuss the quantum-in-cyber risk and its potential impact.

In brief:

- With the advent of cutting-edge advancements in quantum computers and algorithms designed to attack conventional data security mechanisms, organisations are left with no choice but to start recognising the quantum of cyber risk and start mitigation.
- Quantum in cyber risk represents a system-wide, potentially massive impact technology risk, requiring businesses to recognise and quantify this risk for appropriate management.
- Effective risk management involves identifying risk and appropriate owners. It helps prioritise resolution and ensures the appropriate allocation of resources.

Quantum-in-cyber risk is real – inaction is no longer an option

Do you remember Y2K? Many may not even recall how the US spent $100 billion[1] (plus two to three times more globally) preparing for the predicted computing crisis of systems being unable to recognise the year 2000. Experts at the time predicted planes would drop from the sky on the stroke of midnight, while systems would crash and fail across the board. But when the day arrived, there was no catastrophic end to the world as we knew it or very little debate on the Y2K problem ever since.

If quantum-in-cyber risk has the same outcome as Y2K, it will be another job well done for organisations, risk management and technology teams. Quantum-in-cyber risk is the risk presented by the arrival of quantum computers to the encryption algorithms we rely on for cybersecurity today. With Y2K, the world spent billions on an issue that presented an uncertain but potentially catastrophic risk. With quantum computing, we know the storm is coming, and we absolutely need to be prepared. The time is now – we don't have excuses anymore.

Quantum computing poses a known and real threat to modern cybersecurity and, specifically, a threat to all of today's encryption keys that secure the world's most critical systems. Today's most powerful supercomputers would take a billion years (longer than the age of the universe!) to crack the 2048-bit RSA key. This encryption algorithm is de facto a standard for protecting any information from bank statements to health records on the internet. Quantum computers will be able to do this in minutes if not seconds.

Quantum computing algorithms threaten to rewrite the way we protect data as predictions are within 5-15 years, commonly used cryptography algorithms will be broken by quantum computers. In fact, in January of this year, a Financial Times report claimed researchers in China had broken an RSA algorithm – the foundation of many current cybersecurity systems – with quantum computers. Though their claim eventually has not been confirmed but these stories show how close we could be.

EY's Quantum Readiness Survey 2022 found that 81% of senior executives in the UK expect quantum computing to cause industry disruption by 2030. The transformative power and impact of quantum computers is well understood, but what should also be clear is we all need policies in place should we encounter quantum-in-cyber risk.

Unique risk that rapidly scales and spreads

Quantum-in-cyber risk has the potential to be a system-wide technology risk with a massive impact. This makes it different from many other risks currently being managed by organisations. Most technology and cyber risks are associated with a specific system, application or platform. But quantum-in-cyber risks – like Y2K – can and will have a pervasive impact, affecting all platforms and environments, making this an operation-wide issue and a critical risk to the whole business.

Recent reports show that investment in quantum technologies is on the rise, reaching USD 35.5 billion in 2022[2], with 350 quantum computing startups currently in the ecosystem. The big question is how many of today's business leaders are assessing the very real quantum-in-cyber risks?

Lack of awareness among organisations, combined with differing views in public discourse, is one of the largest limitations for any emerging risk, identification, quantification and management. Even among those who have recognised the imminent threat and have attempted to quantify its impact, progress has been limited. The specialised skills required, which are currently limited, have led to a significant proportion of these risks remaining uncharted and unquantified. Systemic/pervasive risk like quantum-in-cyber is also rare – which may require different approaches and skills. This leaves us facing the task of identifying, documenting and quantifying the risk posed by quantum computing in the realm of cybersecurity.

Apply standard risk processes to quantum computing

Organisation that are risk aware, monitor for new and changing risk, quantum-in-cyber is a new and evolving risk. Once it been identified it's important that ownership is assigned to ensure the organisation manages the risk appropriately.

The risk owner is ultimately accountable for risk remediation and allocates resources. This should not be confused with the responsibility of involved teams, that will contribute to an action plan or roadmap to address the risk in their area. Without assigning an appropriate owner, remediation efforts may be inefficient, and the risk may continue to threaten your organisation.

When it comes to identifying risk ownership, there's a simple rule of thumb that can guide you in the right direction. It is derived from risk mitigation strategies. There are only four risk mitigation strategies a company can adopt to deal with a risk: avoid, transfer, reduce or accept. To be considered the risk owner, an individual should have the formal power to take action with regards to the future of the business – be that to **avoid, transfer, reduce or accept** a particular risk. The decision with the most ramifications is usually avoiding the risk, which could potentially mean suspending a line of business or product, along with its IT system or business process. In order to make a decision that would disrupt workflow, the individual must be in a position within the organisation to take this decision or be heard at an appropriate management level. The key to identifying the risk owner is to determine whether they have the power to avoid the risk. If they do, then they are the ones who should take ownership of that particular risk, as they have the proper authority to steer the organisation in addressing the risk.

Let us suppose that the quantum-in-cyber risk is affecting an archive system where HR data is stored. In that case, simple logic may lead to assigning the Archive System owner as the owner of the risk. The system owner may be responsible for some remediation steps but not for the whole risk, as they have no power to decide how or whether to avoid it. The example above highlights a common issue when it comes to assigning a risk owner: who is truly responsible? Some may argue that assigning technology risks to a technology owner is the logical choice, but in many cases it as an irrational approach. The fact that the technology owner is responsible for managing a system and looking after change and audit requests does not automatically make him accountable for risks associated with the system. The better approach would be allocating an ownership role to the head of the HR division, keeping the technology owner responsible for remediation steps.

Business next steps

As the pace of quantum hardware and software development continues to accelerate, quantum-in-cyber risk becomes an ever-present threat to digital systems worldwide. Despite its current obscurity and lack of discussion, this risk has the potential to cause severe damage, making it essential to tackle and proactively manage.

While policy makers, like the National Institute of Standards and Technology (NIST) in the US[3], BSI in Germany[4] or ANSSI in France[5], are working on standardising new encryption schemes that can remain secure in a post quantum world, businesses also have a crucial role to play in bolstering their security. They must begin the journey towards quantum safety. The initial step in this process involves engaging in dialogue about quantum-in-cyber risk and quantifying the potential impact of quantum-in-cyber risk on the organisation's landscape.

Ignoring quantum-in-cyber risk is not an option, as its potential consequences are too great to ignore. Even if an organisation disputes with the severity level of this risk, failure to recognize it puts the entire firm in a less favorable position. The truth is that the risk stays relevant whether it is identified and documented or not. In fact, failing to identify or document a risk can be even more dangerous, as it may go unnoticed and, therefore, unaddressed. Better to be prepared, than to be surprised.

Show references

Related articles

Beyond the hype: a critical look at quantum computing's potential for business and society in Asi...

Explore the significance of quantum computing, and discover its transformative effects and current limitations. Read EY's latest report.

17 May 2023 | **EY Oceania**

Quantum computers will break the existing confidentiality paradigm. The only question is when?

Quantum-in-cyber risk needs attention today

31 Jan 2023 | **EY Global**

Summary

The rapid development of quantum hardware and algorithms presents an ongoing and severe threat to data confidentiality. Although the quantum-in-cyber risk is often overlooked, it has the potential to cause significant harm, making it essential to acknowledge and manage it. Ignoring the risk is not an option, as failing to recognise it can leave organisations in a precarious position. Efficient risk management, where owners of the risk are appropriately chosen and are empowered to fully remediate the risk, could allow to sidestep the most catastrophic outcomes.

About this article

Alexey Bocharnikov
EY Asia-Pacific Quantum Technology Leader

A mastermind of solutions and visionary creator. Quantum technology professional. A skilled athlete, passionate traveler and devoted dad.

Related topics
Cybersecurity