Y2Q: A JOURNEY TO **QUANTUM SAFE CRYPTOGRAPY**

A note on potential largest global migration programs since Y2K

Authors Gireesh Kumar Neelakantaiah • Julian van Velzen • Jerome Desbonnet

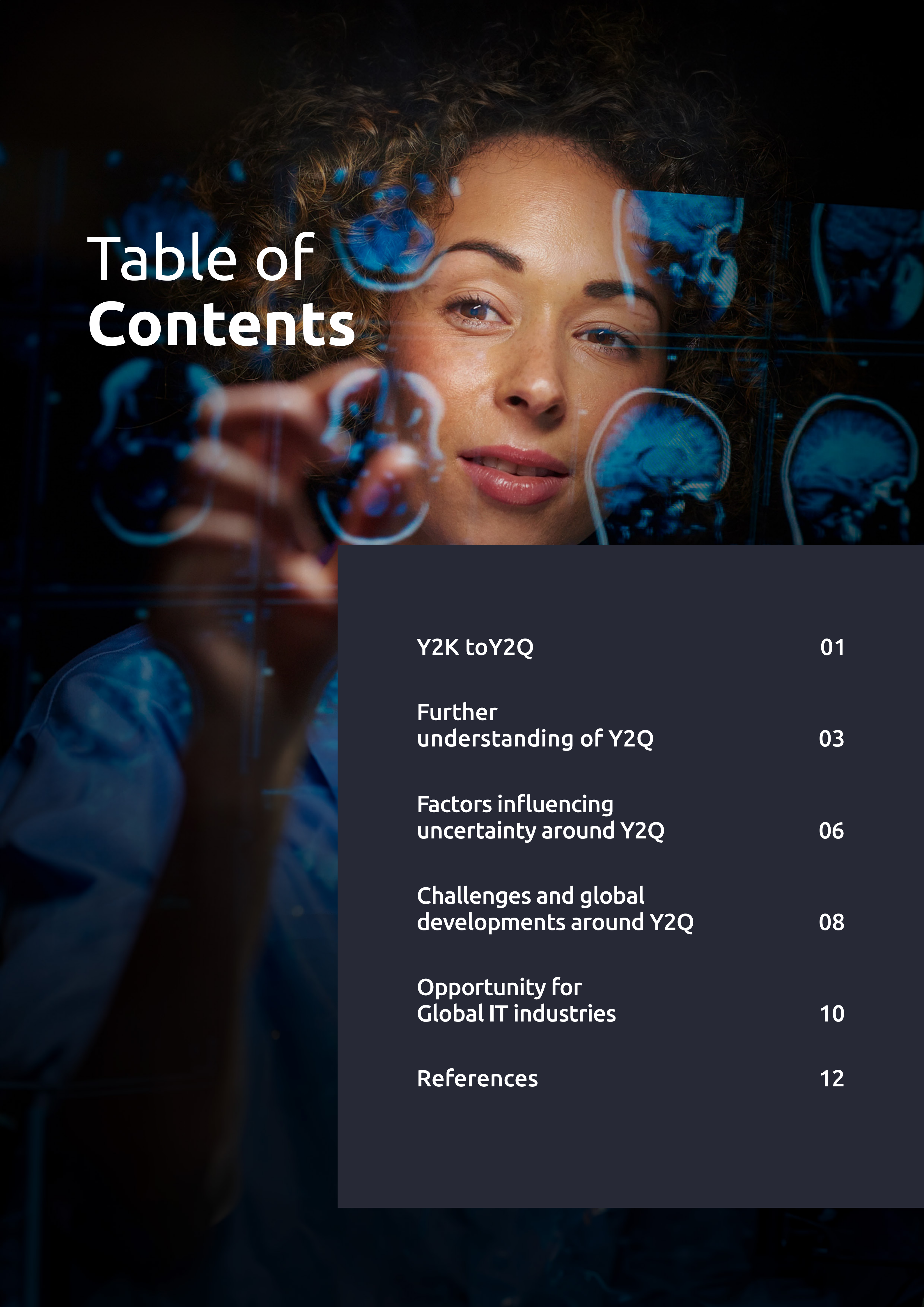

Table of **Contents**

1 Y2K TO Y2Q

Y2K, a quick recap

Almost three decades ago, in 1993 an article titled "Doomsday 2000" got published in Computerworld, describing the Year 2000 problem or Y2K problem which is also known as the Millennium bug. The Y2K issue originated from the 1960s through the 1980s, when memory and disk space was very expensive and limited. Ingenious computer programmers tried to save memory by representing four-digit year values with only the last two digits. But this clever method to save memory led to a serious problem when approaching the end of the century. It was difficult to predict how computer programs would handle year 2000, represented as "00" in computer programs. This potential malfunctioning of computer systems, known as the Y2K bug, caused anxiety among governments and organizations across the world, fearing large scale collapsing of critical systems across sectors in the world. The problem did not only exist in enterprise computers, but also in computers used by factories, utilities, power plants, airplanes and other embedded and operational systems.

Global pre-emptive business continuity efforts were put in place by governments and private organizations to update or upgrade computer systems, addressing the Y2K problem. Many of the governments across the globe established special committees to mitigate the problem and pass specific laws. For example, the US government passed the Year 2000 Information and Readiness Disclosure Act to encourage companies to share their readiness data and to offer them limited liability protection. The solution to this problem was to scan and analyse each line of software programs to either fix or rewrite them. Sounds simple, but it required huge efforts and a profuse number of trained computer engineers to implement the solution.

With international coordination and efforts, the Y2K problem was well addressed, and the beginning of the new century was uneventful. It is estimated that nearly 308 billion USD was spent worldwide, in addressing the Y2K problem with more than 130 billion USD in the US alone.

An Introduction to Y2Q

Let's fast forward to 2023. We are hearing about another similar sounding: the Y2Q problem. The initial seed for this was sown just one year after the publication of the famous Doomsday 2000 article in Computerworld in 1993. The event was the development of the famous Shor's Algorithm by American mathematician Peter Shor in 1994. This is a quantum computer-based algorithm used for integer factorization. The algorithm finds prime factors of an integer in polynomial time, providing exponential speed up, compared to the classical computer algorithms which require super-polynomial times to do the same. This is one of the first and best-known algorithms demonstrating the power of quantum computers.

Before getting into more details of the Y2Q problem, it is necessary to quickly introduce quantum computers, their capabilities, and the current state. Quantum computers are based on the principles of quantum physics. They leverage the principles of superposition, entanglement, and interference to solve computing problems. The fundamental building block of quantum computing is a qubit (short for quantum bit), which is fundamentally different from a classical bit. Because unlike a classical bit, which can be in the state of binary "0" or "1", a qubit can be in a quantum state of "0" or "1" or in a superposition of states "0" and "1" – i.e., at the same time. Quantum computers have the potential to provide an exponential speed-up for certain types of problems when compared to classical computers. The applications of quantum computing are many. Some examples are drug simulation, material science, aerodynamic modelling, supply chain optimization, financial modelling, and many more. Application domains where quantum computers are expected to deliver value can be grouped at a high level, in three areas: optimization, simulation, and machine learning.

The promise of unprecedented computing power to solve current intractable problems is a very attractive proposition for quantum computers. But these quantum computers also have the potential to pose a significant threat to the security of many cryptographic systems that we currently use.

The current cryptography algorithms provide the required security based on complexity of mathematical problems, such as integer prime factorization, which is practically intractable by classical computers. But a sufficiently large and capable quantum computer leveraging Shor's algorithm could potentially perform the factorization task in only hours. This capability can be used to break asymmetric public key cryptographic systems, such as the RSA and Elliptic Curve Cryptography (ECC) algorithms, used in secured communications and digital signature applications. Another quantum algorithm called Grover's search algorithm, could also potentially be used to break symmetric key cryptographic systems, such as the Advanced Encryption Standard (AES), which is used to protect sensitive data. However, the threat of quantum to asymmetric public key algorithms is of the highest.

With quantum computers, actors with malicious intent could potentially break the security of government and enterprise systems, disturb or even damage public services and utility infrastructure, disrupt financial transactions, and compromise personal data. This large-scale threat of the potential ability of quantum computers to crack some of the major cryptographic systems in use today, is referred to as the Y2Q problem.

2 Y2Q - MORE TO EXPLORE

Standard bodies supported by governments and private organizations worldwide are developing multiple quantum safe solutions against the Y2Q problem. Two prominent solutions being proposed are Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

Post Quantum Cryptography (PQC):

National Institute of Standards and Technology (NIST) defines, Post Quantum Cryptography (also referred to as quantum-resistant cryptography) as a development of cryptographic systems that are secure against both quantum and classical computers and can be integrated with existing communications protocols and networks. This consists of a class of asymmetric cryptography algorithms designed to be resilient to attacks by quantum computers. They are still based on classical computing techniques expected to replace today's quantum vulnerable key establishment and digital signature algorithms e.g.: RSA, Diffie-Hellman, and ECC algorithms.

Quantum Key Distribution (QKD):

Quantum Key Distribution is a mechanism for secure communications implementing cryptographic protocols based on principles of quantum physics to enable exchange of keys in most secured manner. Unlike PQC, QDK requires additional hardware for exchanging photonic qubits in free space or over fibre to implement communication system leveraging quantum superpositions and/or entanglements for transmission of quantum states. Communicating parties using QKD can detect any compromise in the communication channel due to eavesdropping as it disturbs the quantum states which can be detected. QKD can be used mainly for exchanging the secret keys and is mostly envisaged to be used along with symmetric key algorithms for secured communication. Though there are some commercial solutions, the technology is still under development.

PQC is expected to be most common form of quantum safe cryptography to be adopted worldwide as they are designed with classical methods and expected to work in the existing infrastructure without need for special hardware, unlike QKD.   Standards and industry bodies are collaborating to develop new quantum safe PQC algorithms. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) is in the forefront of this action and has initiated the process to solicit, evaluate and standardize post-quantum cryptography (PQC) algorithms in 2016. These new algorithms are expected to standardize digital signature, public-key encryption, and key-establishment algorithms capable of protecting sensitive information even after the advent of sufficiently powerful quantum computers. After the third round of evaluation process, NIST has selected four candidate algorithms for standardization.

As per this NIST report published in July 2022, the public-key encryption and key-establishment algorithm that will be standardized is CRYSTALS–KYBER. The digital signature algorithms that will be standardized are CRYSTALS–Dilithium, FALCON, and SPHINCS+. These four selected algorithms are expected to become part of the highly anticipated NIST standards for post-quantum cryptography in 2024.

As the announcement makes clear, these algorithms are designed for two main encryption tasks – the first is general encryption to protect information exchanged over public networks, and the second is digital signatures to authenticate/verify identities. In addition, there are additional candidate algorithms that are being evaluated and the selection of those will be decided by NIST in the fourth round and beyond in the evaluation and selection process.

Similarities and Differences between Y2K and Y2Q

There are some similarities between Y2K and Y2Q. These include:

- Both are triggered by FUD (Fear, Uncertainty and Doubt) based dynamics.
- Both have potential to have large-scale impact on computing and communication systems worldwide.
- Implementation of solution needs a huge number of trained engineers.
- Testing and validation are a very critical part of the solution implementation in both cases.
- There are global efforts and collaboration, across US, Europe, and Asian countries, to address the problem, including involvement of governments. For example, the US passed laws with specific focus on both problems.
- Computer programs and infrastructure across enterprise and operational systems are to be reviewed, assessed, fixed and upgraded in both cases.

Unlike similarities, the differences are more serious with Y2Q, compared to Y2K. For example,

Timelines:

In the case of Y2K, there was a very clear deadline: the beginning of the new century is when the problem would hit the computer systems, if it was not fixed. However, in the case of Y2Q, we do not know when sufficiently powerful quantum computers will be available, which can break currently used cryptography algorithms, thus complete uncertainty of timelines of the threat.

Source of threat:

With Y2K, it was certain that the problem was internally. However, the source of Y2Q is mostly external with malevolent intentions of causing damage/harm.

Solution:

Though Y2K was a huge problem, the solution to solve it was simple and straight forward. To solve the Y2Q problem, there are multiple solutions being proposed. The two key solutions include – Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Each has its own complexity in implementing as a solution. In the near term the recommended solution is implementation of post quantum cryptography.

Execution:

In Y2K, there was a clear deadline before which all systems of an organization had to be updated/upgraded. It was a one-time activity and once the issue was fixed, it was done/solved. But with Y2Q, we need to perform detailed analysis of the systems and data and prepare a roadmap to fix/upgrade the systems considering different priorities like criticality and vulnerability of the systems and shelf life of the data etc. It may end up being a multiyear project. It may not be a one-time activity and organizations need to achieve a state of crypto agility requiring on-going dynamic states of monitor and update cycles.

Visibility of damages:

The potential damages due to Y2K, if not addressed, were expected to be directly visible or noticed. However, with Y2Q the damages may or may not be visible or experienced due to nature of the threat. The malicious agent may not even be revealed immediately and can cause damages at a later point in time.

3 FACTORS INFLUENCING UNCERTAINTY AROUND Y2Q

There is more urgency and anxiety across some industry segments and organizations (especially defense, space, finance, public utilities, and the like) than in others due to different risk profiles. The factors that influence the varying risk profiles and the urgency of different organizations include:

Shelf life of the systems and equipment

Systems and equipment deployed in an organization have a different shelf life. For example, critical infrastructure, vehicles, satellites, intelligent industries, governments, defense, and other hardware equipment with a shelf life longer than 10 years need to be protected on urgent basis, especially over the air (OTA) update related authentications.

Time duration required for migration of the systems

Longer the estimated migration durations, sooner we need to start the journey.

Shelf life of data to be encrypted/protected

The value of data handled and stored by organizations also can have different shelf life. The data considered to be valuable even after 5 to 10 years will need more attention and prioritization than the data with shorter life value. The reason is that the actors with malicious intent could capture and store the encrypted data flowing over the internet today and could decrypt this stored data when large-scale quantum computers become available. This “store now and decrypt later” strategy has become a serious and imminent threat, especially to systems carrying data that has a valid life beyond the anticipated ten years.

Potentially different timelines of threat

Depending on the type of the encryption algorithms used, quantum computing resources required to break them varies. For example, the quantum computing resources required for tackling ECC is less than the resources required for RSA for a given classical security level. In addition, symmetric key algorithms are also vulnerable to Grover's algorithm requiring a much larger quantum computer.

PQC algorithms are new and not proven

The new PQC algorithms selected/shortlisted by NIST are not hardened/proven in the real life environments. Due to this, experts are recommending hybrid approaches (with combinations of traditional and PQC algorithms). These are necessary to be tested in real world applications for functionality and performance. These hybrid solutions, further add to the complexity of implementations. Some leading organizations are already planning to test the candidate algorithms according to their specific use cases.

Fast evolution of quantum systems:

Finally, there are significant investments and efforts going towards improving the performance of quantum computers across all the layers of quantum stack (hardware, control software, algorithms, architecture, and application designs). New algorithms, methods and techniques are being proposed to speed up the journey towards quantum advantage, which could potentially reduce the time available for implementing quantum safe systems.

Considering the above factors, organizations need significant preparation, efforts, and time to implement quantum safe cryptography in their IT and OT landscape. It is better to start the journey soon and understand the risk profile of your organization to prepare suitable roadmap.

4 CHALLENGES AND GLOBAL DEVELOPMENTS AROUND Y2Q

As of today, cryptography management is spread everywhere in the company since we have different workforces managing cryptography at various places such as inside applications, at network level, database layer, and in cybersecurity area. This highlights the fact that it will take huge efforts to assess the risk, quantify it, and mitigate it.

So, what are we missing now? We are missing the ability to express the financial impact on companies and since it's hard to quantify, it's still a bit of an unknown. We know for a fact that quantum risk will have an impact on the insurance premium since there is a risk in the financial communications of the company. Enterprises and governments at least need to start assessing quantum risk since cyber insurance providers will assume the risk to be very high by default. For example, according to CNBC, cyber insurance premiums increased by an average of 28% in the first quarter of 2022, the cyber security premium in France is increasing, and according to Lloyd's, the annual premiums in cyber insurance market will grow from 12 billion USD to 60 billion USD over the next 5 to 10 years. This risk will require the organizations to save and put aside a certain amount, at the end of the year, to mitigate all the financial risk, creating an impact on revenues as well.

This also means that the amount that the companies need to put aside to cover risks is increasing a lot. If enterprises start assessing the risk and are able to prove the impact of risk to be either high, medium, or low as well as taking proactive steps to manage that risk, the cyber insurance providers can be convinced for providing insurance with less premium. So basically, it will have an impact on the amount that is supposed to be provided to the shareholders, the value of the company on the Stock Exchange, and the IPO planning of a company. From a board layer, it means that it will impact the insurance premium, financial results and share value for years. This will be the real impact for enterprises and governments equally and if we don't start preventing quantum risk proactively from today, this impact will keep growing year after year. Furthermore, from 2023 onwards, major insurers will stop nation-backed cyberattacks insurance coverage (quantum threats/attacks are expected to be in the same class). We expect insurance costs related to quantum security to either increase dramatically or not be covered over the next few years.

Also, regulations such as GDPR, California Consumer Privacy Act (CCPA), European Banking Authority, etc. clearly states that data encryption is a way to be protected against fines. Since we know for a fact that quantum computers will break major existing encryptions, it will break protection from legal point of view and invite the burden of non-compliance issues and hefty fines. This will make enterprises either redo everything in emergency situations such as complying with regulations or start preparing right now so that it can be done in a much smoother way without compromising the protection from the regulation standpoint.

Quantum risk in cyber is a growing concern because the materialization of the quantum risk in cyberspace is slowly increasing. However, today's quantum computers are still rudimentary in their capabilities. It will take many years (around ten years based on survey of World Economic Forum with industry experts) for development of powerful quantum computers capable of breaking current security algorithms. However, considering the seriousness of the threat and massive nature of the efforts required, industries, governments, and standard bodies have already started working towards defining standards for algorithms, protocols, and systems that are expected to be secure and resistant to the threats posed by the arrival of large powerful quantum computers.

There have been many global developments recently focusing on quantum technologies and associated risks. For example, issue of National Security Memorandum, Commitment to intensity and elevate cooperation among G7 members to partner and deploy quantum resistant cryptography, release of Requirements of Future Quantum Resistant algorithms for National Security Systems by NSA with 2035 as adoption deadline, publication of post quantum cryptography integration study by The European Union Agency for Cybersecurity (ENISA) and finally passing of Quantum Computing Cybersecurity Preparedness Act.

5 OPPORTUNITY FOR GLOBAL IT INDUSTRIES

Unlike Y2K, there are many uncertainties around Y2Q.
But there are some important developments demonstrating the seriousness and urgency of the problem, for example, passing of Quantum Computing Cybersecurity Preparedness Act by the US government in December 2022, the NSA releasing Quantum Resistant algorithm requirements for National Security Systems with setting expectations for transition to Quantum Resistant algorithms for NSS by 2035, and some insurance companies declaring to end insurance coverage for state cyber-attacks. The organizations across the globe need to recognize these developments. In addition, there has been significant progress happening in the capabilities and performances of quantum computers across all layers – hardware, control software, algorithms and application design and architectures, accelerating the time to quantum advantage.

Governments and private organization have spent an estimated value of 308 billion USD addressing the Y2K problem. As of today, we do not seem to have good/reliable estimates around overall costs of the transition to quantum safe cryptography worldwide. Early estimates indicate that it could be as much as a 1 trillion USD cybersecurity upgrade. But it is very clear that the size and complexity of Y2Q is significantly larger than Y2K and requires solutions over the next couple of decades. It is also necessary to recognize Y2Q as not just a business opportunity, but also as a critical need to secure national interests by adopting quantum safe solutions for systems across governments and private organizations over countries.

Please note Y2Q is beyond the opportunities due to adoption quantum technologies (quantum computing, quantum sensing and quantum communication) across industries.

Another watershed moment for Indian IT industry?

IT industry in India was still nascent in the early 1990s, with 100 million USD in size. Indian IT Industry recognized the huge opportunity around Y2K and started providing trained computer programmers/engineers to help fixing Y2K issues for clients across the globe and hundreds of companies, with thousands of jobs, created in this process. It was a watershed moment for the industry in India and by the end of the century the Indian IT exports reached nearly

8 billion USD. This also provided the much-needed opportunity and recognition for the industry and helped building strong foundations of the IT services export business in India. The global Y2K problem provided the launchpad for the Indian IT industry to scale new heights in the coming years. In the following two decades, as per NASSCOM report, Indian IT industry had very good growth and reached a size of around 227 billion USD by 2022.

During the Y2K problem, the Indian IT industry was still in its early stages and acted as a low-cost labour centre, providing trained engineers to implement a relatively simple solution. Now the Indian IT industry has grown to more than 200 billion USD and is recognized as a leading force worldwide, capable of delivering advanced digital and technical solutions to its global clients. In addition, India has strong academic and research institutions around quantum technologies, enabling development of innovative solutions for both PQC and QKD solutions. With this capability, the Indian IT industry can take a lead position providing innovative solutions to Y2Q problem, which is complex and needs significant thought leadership.

Looking at the size and nature of this opportunity, the key question is: How ready is the IT industry and more specifically will the Indian IT industry take the leadership role in providing solutions to Y2Q, creating another watershed moment for the IT industry?

6 REFERENCES

1. https://en.wikipedia.org/wiki/Year_2000_problem
2. https://nasscom.in/knowledge-center/publications/technology-sector-india-2022-strategic-review
3. https://www.livemint.com/Opinion/fNjocJ9cwlGCDqLWt2OjXP/Indian-IT-and-ITeS-journey-Liberalization-and-beyond.html
4. https://quantumconsortium.org/quantum-safe-guide/
5. https://www.sciencedirect.com/science/article/abs/pii/S0268401298000437
6. https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future
7. https://www.congress.gov/bill/117th-congress/house-bill/7535
8. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
9. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
10. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
11. https://www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf
12. https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
13. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get The Future You Want | www.capgemini.com