Adoption of Post-Quantum Cryptography in Organizations: Challenges and Drivers

Daniel Zimmermann

Dissertation written under the supervision of professor Peter V. Rajsingh PhD

Dissertation submitted in partial fulfilment of requirements for the MSc in Business, at the Universidade Católica Portuguesa, 19.03.2025.

Abstract

The emergence of quantum computing poses a significant threat to modern encryption standards, with the potential to render widely used cryptographic protocols obsolete. To mitigate this risk, organizations must transition to post-quantum cryptography (PQC), a process that requires technical, operational, and strategic adjustments. However, the pace and approach to adoption vary across industries and organizational size, influenced by both external pressures and internal capabilities.

This study employs a mixed-methods approach, incorporating 14 expert interviews and survey responses from 37 cybersecurity professionals to examine the factors driving and inhibiting PQC adoption. The findings reveal that while regulatory mandates play a role, organizations are increasingly guided by risk exposure and reputational concerns. Key challenges include resource constraints, reliance on third-party vendors, and the complexity of cryptographic inventory assessments and legacy systems. Despite these challenges, the study found that PQC adoption will accelerate as risk awareness grows and implementation guidelines become available. It emphasizes the importance of a strategic, resilience-focused approach to cybersecurity, incorporating cryptographic agility, continuous assessments, and hybrid encryption solutions to navigate the evolving threat landscape.

Keywords: Quantum Computing, Cybersecurity, Post-Quantum Cryptography, Risk Management, Cryptographic Agility, Technology Adoption, Dynamic Capabilities

Title: Adoption of Post-Quantum Cryptography in Organizations: Challenges and Drivers

Author: Daniel Zimmermann

Resumo

A computação quântica representa uma ameaça significativa aos padrões modernos de encriptação, com o potencial de tornar obsoletos os protocolos criptográficos amplamente utilizados. Para mitigar esse risco, as organizações devem adotar a criptografia pós-quântica (PQC), um processo que exige ajustes técnicos, operacionais e estratégicos. No entanto, o ritmo e a abordagem da adoção variam conforme o setor e o tamanho da organização, influenciados por pressões externas e capacidades internas.

Este estudo adota uma abordagem de métodos mistos, com 14 entrevistas a especialistas e um inquérito a 37 profissionais de cibersegurança, para analisar os fatores que impulsionam e dificultam a adoção da PQC. Os resultados indicam que, embora os requisitos regulamentares sejam relevantes, a exposição ao risco e preocupações reputacionais são fatores determinantes. Os principais desafios incluem restrições de recursos, dependência de fornecedores externos e a complexidade da avaliação de inventários criptográficos e sistemas legados. Apesar dessas barreiras, a adoção da PQC deverá acelerar com o aumento da consciencialização sobre riscos e a disponibilização de diretrizes de implementação. O estudo destaca a importância de uma abordagem estratégica e resiliente, incorporando agilidade criptográfica, avaliações contínuas e soluções híbridas de encriptação para enfrentar um cenário de ameaças em evolução.

Palavras-chave: Computação Quântica, Cibersegurança, Criptografia Pós-Quântica, Gestão de Risco, Agilidade Criptográfica, Adoção Tecnológica, Capacidades Dinâmicas.

Título: Adoção da Criptografia Pós-Quântica nas Organizações: Desafios e Impulsionadores

Autor: Daniel Zimmermann

Acknowledgments

Throughout this journey, I have been fortunate to receive support from many individuals, to whom I would like to express my gratitude. First and foremost, I am deeply thankful to my supervisor, Prof. Peter V. Rajsingh, for his guidance, support and responsiveness which were instrumental in shaping this dissertation.

I am also sincerely grateful to the 14 experts who generously shared their time and insights, enriching this dissertation with invaluable perspectives. Likewise, I extend my thanks to the 37 industry professionals who took the time to complete my survey, as well as those who facilitated warm introductions and referrals, enabling me to reach a broader network.

A special thanks goes to my family, whose unwavering support has been a constant source of strength and stability. I am equally grateful to my friends, who have enriched my life during this journey, keeping me motivated and inspired.

Lastly, I would like to acknowledge the many acquaintances that colored the many places I had the privilege of exploring in the meantime. These experiences have not only broadened my perspective but also made this period one of the most memorable times of my life.

Daniel

Table of Contents

List of Figures

List of Tables

List of Abbreviations

PQC - Post-Quantum Cryptography

DDoS - Distributed-Denial-of-Service

SNDL - Store Now, Decrypt Later

RSA - Rivest, Shamir, Adleman encryption

ECC - Elliptic Curve Cryptography

IoT - Internet of Things

SME - Small & Medium Enterprises

ERM - Enterprise Risk Management

NIST - National Institute of Standards & Technology

AES - Advanced Encryption Standard

SHA - Secure Hash Algorithms

PoW - Proof-of-Work

SVP - Shortest Vector Problem

CVP - Closest Vector Problem

QKD - Quantum Key Distribution

CRQC - Cryptographically Relevant Quantum Computer

TAM - Technology Acceptance Model

PU - Perceived Usefulness

TLS - Transport Layer Security

DES - Data Encryption Standard

QC - Quantum Computing

DH - Diffie Hellman key exchange

VIF - Variance Inflation Factor

1. Introduction

In today's rapidly technologically advancing world, digitization is increasingly integrated into nearly every aspect of life. From E-commerce, finance and healthcare, to infrastructure and the internet of things powering modern smart cities, digital developments in these sectors are elevating the economy and quality of life (OECD, 2019). However, digitalization also increases the number of data touchpoints and potential vulnerabilities which simultaneously amplifies exposure to the threat of cybercrime. The potential for severe damage, not only in economic measures but also to individual privacy and national security, underscores the importance of maintaining resilient cybersecurity to safeguard against increasingly sophisticated cyber threats (Pescaroli et al., 2018). While current efforts are focused on mitigating established threats such as Ransomware and Distributed-Denial-of-Service (DDoS) attacks, technological advancements in quantum computing are introducing a threat potentially disruptive to the entire cryptographic foundation that modern digital security is built upon (Raban & Hauptman, 2018).

Once they become prevalent, quantum computers will theoretically be able to break many of the encryption algorithms that are currently implemented, essentially threatening the integrity of most of today's data privacy and security infrastructure. Some organizations are already at risk today, as "store now, decrypt later" (SNDL) schemes threaten information with extensive confidentiality lifetimes (Mosca, 2015). Meanwhile, cryptographers have developed new algorithms that are considered quantum-secure and recently released the first set of standards (NIST, 2024c). Facing an uncertain timeline in quantum-computing development, as well as historic evidence of lengthy implementation procedures for new standards, businesses are challenged with balancing the urgency of cryptographic system overhauls with associated operational challenges and transition costs (Learner et al., 2023).

The current academic literature is limited on the drivers and barriers of quantum-safe encryption, a gap this thesis aimed to fill. The Research Question is: **What factors are influencing adoption of post-quantum cryptography?**

This dissertation begins with a literature review of the fundamentals of cybersecurity and quantum computing, explores the impact of quantum advancements on cybersecurity, and provides an overview of related management theory. The research design and data collection of expert interviews and surveys are presented in the subsequent methodology, followed by

the analysis and discussion of the research question. Finally, the theoretical and practical implications are concluded, including limitations and opportunities for future research.

2. Literature Review

This section explores the current state of the cybersecurity field, the technology of quantum computing, and their intersection. In particular, we discuss how quantum computing will disrupt modern information security and what emerging solutions can protect sensitive data in the future. By outlining potential threats and approaches for mitigation, along with associated challenges for adoption and implementation, we review the evolving landscape towards post-quantum cyber security.

2.1. Cyber Security

2.1.1. Introduction to Cryptography

For millennia, cryptography has been fundamental to securing information and its exchange by scrambling a source plaintext into an unintelligible ciphertext via an encryption method that only allows for decryption by parties possessing the correct key. The earliest documented ciphers date back to the fifth century B.C. where the Spartans encrypted messages using specific diameters of wooden staffs, around which leather strips were wound during composition and decryption. Julius Caesar extensively used ciphers involving alphabetic substitution, known as the Caesar Shift Cipher. This shaped cryptography for the millennia to come until the method of frequency analysis, first discovered by Arabic scholars, became popularized in Europe and rendered codes breakable (Kotas, 2000).

During the world wars, the strategic necessity of secure communications drove advancements in cryptography and led to sophisticated developments like the purple machine and the Enigma. Yet, human errors of repetitive usage patterns allowed the mathematician Alan Turing famously to crack the Enigma code using even more sophisticated machines, thus pioneering computer technologies in the process. In the 1970s with the advent of computers, encryption evolved into the digital realm. IBM's "Lucifer" was the strongest commercial cipher at that time and became the U.S. encryption standard in 1976. However, the problem of key distribution, which was only truly secure through physical (symmetric) exchange, posed scalability issues for the globalizing trajectory of digital connectivity (Kotas, 2000).

To address this problem, Diffie & Hellman (1976) introduced the concept of an asymmetric cipher using separate keys: a public one for encryption and a private one for decryption. Ron Rivest, Adi Shamir and Leonard Adleman developed an algorithm for practical

implementation in 1977. Their encryption method relied on a “one-way” or “trapdoor” function, which involved an easy computation that was difficult to revert. More specifically, information would be encrypted by a sender using the publicly displayed multiplied product of a recipient’s private and public keys, which can only be decrypted using the recipient’s private key. The security of this algorithm hence relies on the mathematical difficulty of the factorization problem in finding the large prime numbers (keys) making up the cipher. With the computational capacity available then, the factorization of a 200-digit number was estimated to take $3.8\ x\ 10^9 = 3{,}800{,}000{,}000$ years to compute (Rivest et al., 1978). This cypher, named after its developers’ initials (RSA), was a breakthrough for secure encryption without requiring physical key exchange. It formed the basis of all modern age digital encryption (Merkle, 1980).

Incremental key-size adjustments have been made throughout the years to keep up with advances in hardware and software capabilities (Althobaiti & Dohler, 2020). After an RSA key with 1024 bits was broken in 2010, the minimum recommended key size was been raised to 2048 bits (Pellegrini et al., 2010). A significantly more efficient evolution based on Elliptic Curves (ECC) introduced a new standard in 1999 and found early adoption especially in resource constrained applications. However, it has only recently replaced RSA as the most widely used encryption method (Joseph et al., 2022). While these standards are still considered secure, the cyberspace has still faced malicious activity, as methods beyond code-breaking have emerged, mainly exploiting flaws in human behavior (Eling & Wirfs, 2019).

2.1.2. Current Threat Landscape

As modern society becomes increasingly digitized and technologically interconnected, with growing reliance on the internet and autonomous technologies, complex networks of digital interfaces and critical infrastructure, and vast amounts of stored data on individuals and organizations (Koops, 2016), the elevated level of exposure to cyber threats significantly increases the risk of catastrophic outcomes (Pescaroli et al., 2018). Among the most critical domains are financial and healthcare institutions, infrastructure such as telecommunications, energy grids and water supply, and databases storing sensitive personal, governmental and military data, posing attractive targets especially for state-sponsored attacks. (Li and Liu 2021, Kang et al., 2015). The proliferation of the Internet of Things (IoT), which powers intelligent systems like smart cities, smart homes and Industry 4.0, adds additional layers of

vulnerabilities (Alaba et al., 2017). The amount of operational IoT devices is estimated at around 20 billion in 2025 and projected to double by 2033 (Statista, 2024).

The most significant cyber threats include (ENISA, 2024; Mijwil et al., 2023):

- *Social Engineering*: initial access through human deception (e.g. phishing)
- *Ransomware*: extortion by encryption of data or threat of data disclosure.
- *Other malware*: viruses, data bombs, trojan horses (Li & Liu, 2021)
- *Denial of Service*: system resource exhaustion to limit access (e.g. DDoS)

Some cyber-attacks indiscriminately scan for vulnerabilities across a wide range of systems, while others, like Advanced Persistent Threats (APT), focus on targets with more sophisticated defenses and deploy a range of long-term strategies to achieve a successful breach (Che Mat et al., 2024).

To illustrate the impact of these threats, famous examples of large-scale cyberattacks include the WannaCry ransomware attack in 2017 which impaired numerous organizations worldwide, including UK health care institutions, and amounted to an estimated loss of US$8 bn (Parenty & Domet, 2019; Weintraub & Borenstein, 2017). Similarly, the NotPetya malware attack in the same year infiltrated Windows systems globally and inflicted US$10 bn of damage (GAO, 2021). Yahoo suffered the historically largest data breaches in 2013 & 2014, with sensitive information stolen from over 3 billion affected user accounts (Hallenbeck, 2024). Examples for attacks on critical infrastructure include the ransomware attack on the Colonial Pipeline in 2021 which shut down delivery of 2.5 million barrels of fuel per day, leading to supply chain disruptions of several days (McCormick & Brower, 2021), and the malware attack on the Ukrainian power grid in 2015, causing outages that affected 225 thousand customers (CISA, 2021).

As cybercriminal tactics evolve to exploit emerging vulnerabilities, the frequency and financial consequences of cybercrimes have surged, and rank as the top business risk in 2024 according to Allianz (2024). Between 2018 and 2020, the economic costs of cybercrime have increased from 600 bn US$ (Lewis, 2018) to 1 trillion US$ annually (Lewis et al., 2020), and as of the year 2024, the European Union estimates global annual cybercrime costs at €5.5 trillion (EU, 2024). Risks for organizations range from financial losses and breaches of sensitive information like IP and trade secrets to operational disruptions and even potential human safety hazards (Lezzi et al., 2018). A significant contributor to the risk of large-scale attacks are monocultures in the soft- and hardware markets, such as third-party cloud services

that enable widespread accumulative damage (Eling & Schnell, 2020). In industries with robust security standards, a shift of attack patterns towards more vulnerable supply chain partners has become evident (Zeller & Scherer, 2022). SME have also experienced an increase in attacks as budget constraints don't allow for cyber security on par with larger corporations (Goldman Sachs, 2019). The Ponemon Institute reported a 15% rise in the average cost of a data breach, from US$3.86m in 2018 to US$4.45m in 2023. Recently, the cost surged by an additional 10%, amounting to US$ 4.88m in 2024, mainly incurred by lost business and post-breach responses (IBM & Ponemon, 2018; 2024).

2.1.3. Cyber Solutions

To offer protection services against cyber-attacks, the cyber security industry has co-evolved with the threat landscape and developed defense systems such as firewalls, antivirus and intrusion detection software (Mijwil et al., 2023). In 2024, the largest three industry players covered a broad range of threats in a mix of service offerings. Palo Alto Networks is the current leader (market cap US$120 bn), followed by CrowdStrike (market cap US$72 bn) and Fortinet (market cap US$61 bn). Additionally, some companies focus on specialized threats, such as Cloudflare (market cap: US$30 bn) in mitigating DDoS attacks. Global market growth is projected to almost triple from US$194 bn in 2024 to US$563 bn by 2032 (Fortune Business Insights, 2024a), signifying the growing economic risk of compromised digital assets.

Despite sophisticated preventive measures, the evolving nature of cybercrime continues to expose organizations to exploitable vulnerabilities. To mitigate this risk, cyber risk insurance has become a crucial component of comprehensive risk management strategies. Established risk management frameworks such as COSO ERM categorize risks into operational, reporting, compliance and strategic risks, providing organizations with a structured approach to address diverse threats. While implicating all these categories, cyber risks are generally defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems" (Cebula et al., 2018) due to their immediate impact on systems and processes. As various indirect cleanup costs such as incident investigation, crisis management, regulatory and industry sanctions, class action lawsuits, and opportunity costs can accumulate, cyber insurance helps in minimizing damage, liability and performance issues (Algarni et al., 2021;

Eling, 2020). Industries that store large amounts of personal data, such as healthcare and retail, or rely on digitalized processes, like manufacturing and telecommunications, are among the most frequent purchasers of cyber insurance (Zeller & Scherer, 2022).

The global cyber insurance market is valuated at US$14 bn in 2023 and projected to double to US$29 bn by 2027, emphasizing its significance to cybersecurity risk management (Munich Re, 2024). Despite this growth, a large gap remains between cyber insurance coverage and the actual value of assets at risk of impairment, on the magnitude of US$ trillions.

While there is no shortage of demand for cyber risk transfer through insurance, cyber risk management has not reached levels of maturity seen in other forms of organizational risk management, primarily due to the complexity of quantifying the risks involved (Zeller & Scherer, 2022). The common practice within Enterprise Risk Management (ERM) is to measure impact and probability of different types of risks, and allocate resources in accordance with the board's risk tolerance (Stine et al., 2020). As many affected companies refrain from disclosures, the availability of public historical data on cyber incidents remains limited (Eling et al., 2023). On top of the fast evolving nature of cyber threats, there is disparity of data protection laws and heavy tails risks due to intangible damages (Dacorogna & Kratz, 2023). Hence, establishing appropriate pricing and coverage becomes complex to quantify accurately (Zängerle & Schiereck, 2023) (Zeller & Scherer, 2022) (Eling et al., 2023). Facing these uncertainties, cyber insurers tend to overprice coverage (Kshetri, 2018), further complicating risk management strategies.

Despite the rising stakes of negligence, many organizations struggle to allocate sufficient budgets for cybersecurity, as it is generally not perceived as an imminent contributor to organizational value in comparison with business expansion or revenue generating projects (Ashby et al., 2018; Pooser et al., 2018). Hence, cybersecurity strategy is typically driven by the regulatory environment with a compliance mindset (White & Caralli, n.d.). For example, the EU General Data Protection Regulation (GDPR) framework imposes heavy sanctions on data breaches, with penalties amounting to €20 million or 4% of global turnover, whichever higher (GDPR.EU, 2018). MunichRe, the world's largest reinsurance company and cyber risk insurer, reported 83% of their interviewees not being adequately protected against cyber threats (Dacorogna & Kratz, 2023). To address these vulnerabilities, organizations must focus on building cyber resilience, defined as "the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015). This involves not only preventative measures but also strategic investments in data governance, incident response

plans, and employee training, all of which have proven to reduce financial impacts of breaches by containing attacks and ensuring fast recoveries (IBM & Ponemon, 2024).

2.2. Quantum Computing

2.2.1. Introduction to Quantum Computing

Quantum computers have been in development since the 1980s when the theoretical physicist Richard Feynman published "Simulating physics with Computers" (Feynman, 1982). Built upon the principles of quantum mechanics, quantum computers harness the phenomena of superposition, interference, and entanglement to solve complex problems (Mind Commerce, 2020). In contrast to classical computers, which perform consecutive operations using digital bits that can only exist in one state at the time - 0 or 1 (Althobaiti & Dohler, 2020), quantum bits can exist in both states at the same time – a superposition of 0 and 1 – and perform simultaneous calculations. This provides a computational edge to digital bits for handling exponentially larger data sets and combinatorial problems with numerous states or outcomes more efficiently (Mind Commerce, 2020). To illustrate, given that n qubits represent 2^n states simultaneously, merely 30 qubits would already allow for $2^{30} = 1{,}073{,}741{,}824$ simultaneous calculations. At 300 qubits, the amount already jumps up to $2^{300} = 2.037..x\ 10^{90}$, which is more than the number of particles in the observable universe.

The challenge lies in harnessing the inherently unstable probabilistic nature of quantum mechanics for practical applications, requiring the use of stochastic methods and highly controlled conditions to mitigate error and decoherence (Wang, 2012). There are different structural approaches to building quantum computers, including the use of electrons, photons and trapped ions. The most popular are silicon-based, superconducting circuits due to scalability and compatibility with current manufacturing capabilities, as used by pioneering companies like IBM and Google (Mind Commerce, 2020).

2.2.2. Current State of Research

Although significant advances have been made in recent years, quantum computing is still in its early stages. The American National Institute of Standards and Technology (NIST) created the first quantum chip in 2009 (Lewis & Wood, 2023). Since then, major tech companies such as Alibaba, IBM, Amazon, Google, Intel, Toshiba, Honeywell, Nvidia and Microsoft, along

with specialized companies like Quantinuum and PsiQuantum have been invested in the effort to capture a share of the estimated market size of US$50 bn by 2030 (KPMG, 2024). In 2019, Google achieved a major milestone by demonstrating quantum supremacy using its 53 qubit "Sycamore" processor, proving that quantum computers are already equipped to solve problems beyond the capabilities of classical computers by completing a task in 200 seconds that would take a state-of-the-art supercomputer 10,000 years (Acharya et al., 2023; Arute et al., 2019). Currently leading the race, IBM has been making developmental leaps, releasing a 127-qubit chip in 2021, a 433-qubit chip in 2022 and achieved the latest breakthrough of a 1,121-superconducting-qubit chip in 2023 (Castelvecchi, 2023), indicating exponential growth. Partnering with Japan's National Institute of Advanced Industrial Science and Technology (AIST), a 10,000-qubit quantum computer is planned for 2029 (Swayne, 2024) and by 2033, the company aims to build a 100,000-qubit system (IBM, 2023).

Despite these advancements, the technology still faces significant physical challenges. Quantum states are highly unstable and prone to errors, requiring a vacuum and cryogenic cooling to absolute zero (-273°C) to eliminate environmental disturbance and maintain stability for a sufficient duration to perform useful computations (Castelvecchi, 2023). Even the best systems still run on imperfect qubits and require validation of result accuracy, directing the majority of current research efforts towards the creation of fault-tolerant qubits and error correction improvements (Dwivedi et al., 2023). This is achieved by bundling multiple physical qubits to represent a single logical qubit with higher stability and accuracy (Castelvecchi, 2023; Mind Commerce, 2020). IBM's recent release of a 133-qubit chip (Heron) with record-low error states, and discoveries of alternative error-correcting methods like the quantum low-density parity check (qLDPC) show progress in further improving qubit performance (Bravyi et al., 2024).

2.2.3. Applications

Quantum computing is expected to revolutionize industries by accelerating scientific research, particularly in fields such as molecular physics, materials- and data science. However, the driver behind the global race has been the potential of breaking the majority of established public key encryption schemes, which poses profound implications for national security (Mind Commerce, 2020). Determined to achieve a competitive edge, governments are heavily investing in this technology. China is leading the effort with US$15.3 bn invested in 2023

whilst running the world's largest quantum research facility in Hefei (Learner et al., 2023). As of 2022, the US has allocated US$2.9 bn and seen private sector investments of US$3.7 bn, the European Union US$1.1 bn with projected additional US$7.5 bn, and the UK US$1 bn with projected US$3.1 bn (Lewis & Wood, 2023).

Considering the required investments into specialized infrastructure and hardware, as well as high maintenance costs, quantum computers are generally not feasible for personalized desktop use. However, by utilizing cloud infrastructure, remote access to quantum computational resources can be provided "as-a-service", as already adopted by universities for research (Lewis & Wood, 2023). Furthermore, quantum computers are specialized machines that cannot be updated via software like classical computers. Instead, they require physical modifications to run specific algorithms. For general computing tasks, they will remain subservient to classical computers which run superior clock-speeds. Hence, business models will likely focus on Infrastructure-as-a- service, hardware-as-a-service, managed service and component as a service models (Mind Commerce, 2020). Despite ambitious growth projections, the quantum computing market size in 2024 is estimated at merely US$1.16 bn, reflecting the industry's nascent stage of commercialization (Fortune Business Insights, 2024b).

2.3. Implications of Quantum Computing on Cyber Security

2.3.1. Threats to Cyber Security

While the cybersecurity and cyber insurance industries focus on currently established threats, advancements in quantum computing impose unprecedented implications on the cryptographic foundation of modern information security. The edge of quantum computers in performing vast amounts of simultaneous computations poses a direct threat to today's widely implemented encryption standards like RSA and ECC (NIST, 2023), which rely on the difficulty of combinatorial mathematical problems like the factoring of large numbers. While these would take classical computers millions of years to solve, a sufficiently powerful quantum computer could solve them in seconds (Althobaiti & Dohler, 2020). To illustrate the extensive range of security products affected, EY (Gilkes, 2023) has listed the following examples: Public key infrastructure, secure software distribution, federated authorization, key exchange over public channel, secure e-mail, virtual private network, secure web browsing and controller devices.

Two algorithms were developed near the end of the 20th century which may empower quantum computers to break modern encryption exponentially faster, threatening the security of all of cyber space:

Shor's refactoring algorithm (1994):

Run on a sufficiently powerful quantum computer, this algorithm would be able to break the current standard 2048-bit RSA asymmetric public key cipher. While the initially estimated number of required qubits to perform this operation within 8 hours was one billion in 2015, this number has dropped in 2019 to 20 million (Gidney & Ekerå, 2021), indicating high levels of ambiguity around projections. Other research suggests that as little as approximately 4,000 logical qubits could suffice (Roetteler et al., 2017), and a paper from 2021 claims to require merely 13.5 thousand physical qubits to crack 2048-bit RSA in 177 days (Gouzien & Sangouard, 2021).

Grover's quantum search algorithm (1996):

This algorithm enables a quadratic acceleration of unstructured search problems, enhancing quantum computer capabilities to perform brute-force attacks on symmetric encryption like AES and hash functions like SHA (Dwivedi et al., 2023). *Hash functions* convert any length of plaintext to a unique, fixed length ciphertext or "digest" (in the case of SHA 256 the length is always 256 bits) which is mathematically impossible to revert. Hence, a hash does not store encrypted information, but instead functions as its unique identifier or fingerprint for use cases like password validation, digital signatures or blockchains (Preneel, 2005). Grover's algorithm threatens these encryption methods by increasing the efficiency of finding and matching the correct key or input in an unsorted dataset. Although not as critically impactful as Shor's, as increases in key or hash sizes sustain adequate security, the implications are rooted in the added computational resource requirements (Chen et al., 2016).

Example of implications on Blockchain

Blockchain is a decentralized ledger technology that securely records and verifies transactions across a network of computers. It is built upon a public ledger, essentially a sequential history of transactions or blocks which are linked together through cryptographic hashes, forming a chain of references to ensure its integrity. Any party (miner) possessing sufficient computational power may contribute blocks to the ledger by performing a "proof-of-work" (PoW), which is a consensus mechanism involving the solving of a complex mathematical problem, intentionally slowing processing time to allow the entire network to record and validate the transaction (Fedorov et al., 2018). The security of the blockchain relies on no

entity controlling more than 50% of the computational power, which would otherwise allow for a system hijack and the creation of an alternative history of transactions (Aggarwal et al., 2018).

For Bitcoin, PoW takes the network on average 10 minutes to solve (Nakamoto, 2008). Using Grover's search algorithm (Grover, 1996), a quantum computer with a gate speed of up to 100 GHz could solve the PoW 100 times faster than current technology (Aggarwal et al., 2018) and hence perform a so-called 51-percent attack by controlling the majority of the network's computing power, sabotaging other parties' transactions or obscuring transactions from being recorded in the blockchain (Kiktenko et al., 2018). In addition, blockchain transactions on most platforms are authorized using digital signatures based on elliptic curve cryptography or RSA, which are vulnerable to Shor's algorithm (Holmes & Chen, 2021) (Witte, 2016) (Fedorov et al., 2018).

2.3.2. Emerging Solutions

To address this emerging threat, government, academia and industry have come together in a public-private partnership to develop quantum-safe algorithms that could withstand attacks from quantum computers once they achieve levels of cryptographic relevance. In 2016, the U.S. National Institute of Standards and Technology (NIST) launched a global effort to collect, test and eventually release new algorithm standards for a post-quantum era (NIST, 2016). Of the initial 69 submitted algorithms, 3 have been recently approved as standards (NIST, 2024c):

- ML-KEM (Module-Lattice-based Key-Encapsulation Mechanism) is a lattice based algorithm for **key-establishment** (NIST, 2024b)
- ML-DSA (Module-Lattice-based Digital Signature Algorithm) is a lattice based algorithm for **digital signatures** (NIST, 2024a)
- SLH-DSA (Stateless Hash-based Digital Signature Algorithm) is based on hash functions as a non-lattice alternative for **digital signatures** (NIST, 2024d).

Lattice-based algorithms are currently considered among the most secure defenses against quantum attacks. They rely on mathematical structures called lattices, which "are sets of points in n-dimensional spaces with a periodic structure" (Fernandez-Carames, 2020), in which a point containing information is hidden with the addition of random noise (Bernstein & Lange, 2017). Encryption is secured through the problem of finding the optimal vectors

(the keys) to reach the closest lattice to the hidden point, which is NP-hard (NP = nondeterministic polynomial time) even for quantum computers (Ajtai et al., 2001; Peikert, 2009) and increases in difficulty by scaling the number of dimensions. Figures below (Mansoor et al., 2024) illustrate the shortest vector problem (SVP) and closest vector problem (CVP) in a simplified manner, whereby $b1$ & $b2$ represent the n-vectors defining the lattice grid and the problem to be solved is displayed in red. The SVP involves finding the shortest nonzero vector within a multidimensional lattice, whilst the CVP involves a given vector (green) to which the closest lattice point is to be found.

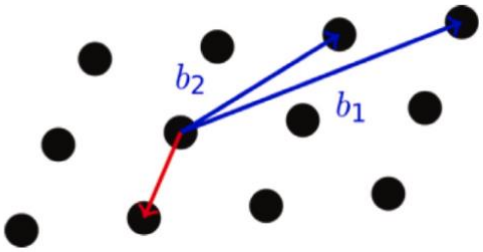

Figure 1: Shortest Vector Problem (SVP)

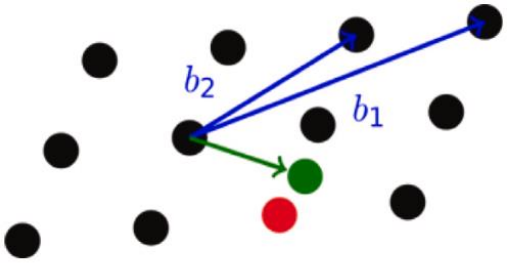

Figure 2: Closest Vector Problem (CVP)

While the new standards offer promising alternatives, they require longer keys and processing times than current algorithms (RSA, ECC) and each have specific tradeoffs in suitability for specific applications, rendering the implementation process less straightforward (World Economic Forum, 2022). Furthermore, the full scope of quantum threats remains uncertain and most algorithms have yet to stand the test of time (Ott et al., 2019).

While quantum mechanics pose a threat to information security, they can also enhance it through a truly secure method for key exchange over a distance known as Quantum key distribution (QKD). Since quantum states collapse during measurement, eavesdroppers are unable to intercept undetected, ensuring information-theoretic security - meaning no algorithm can be developed for a third party to access the exchanged keys (Dwivedi et al., 2023). Some cyber security companies have specialized in this technology, pioneered by Swiss-based IDQuantique in 2001. However, widespread adoption of this technology may be limited due to the cost and complexity of implementation, requiring physically connected optical fiber channels to every node in the network and hence limiting range to merely tens of kilometers due to photon losses (Fedorov et al., 2018). This technology requires extensive

infrastructure investment into networks of quantum satellites and repeaters to become feasible (Pirandola et al., 2020) (World Economic Forum, 2022).

2.3.3. Implementation Timeline and Challenges

Although the new post-quantum cryptographic standards have been released, their widespread adoption anticipates a lengthy process. History shows that implementing new cryptographic standards can require decades across industries (Barker et al., 2021). The ECC was proposed in the 1980s and demonstrated superior efficiency to RSA requiring about one-tenth the key size for comparable security, yet it only found widespread adoption two decades later (Joseph et al., 2022). Considering the billions of embedded systems and legacy IoT devices which lack appropriate computational resources, updating processes is difficult, if not impossible, to effect. The vast scale of existing cryptographic infrastructure will demand substantial investment for quantum-safe migration (Fernandez-Carames, 2020; Ott et al., 2019).

In the example of blockchain, the performance implications of longer keys on processing times for quantum-safe cryptographic algorithms pose significant adoption barriers for currently established decentralized blockchains, which require a broad consensus to be implemented and don't address the 51% attack threat of dominating the network (World Economic Forum, 2022). A better solution would be the migration to new quantum-resistant solutions (Holmes & Chen, 2021), as have been proposed by various researchers to include the use of lattices (Zheng, 2024) or even quantum mechanics (Jogenfors, 2019) (Rajan & Visser, 2019).

To facilitate the transition, intelligence, standardization and consulting institutions are advocating building a quantum-readiness roadmap for achieving crypto agility (CISA et al., 2023) which describes the ability of a system to update and replace cryptographic components with minimal disruption (Alnahawi et al., 2023). In fact, US federal agencies are mandated to achieve quantum-security by 2035 (Moody et al., 2024). Many organizations lack this capability due to incomplete cryptographic inventories, making it harder to assess vulnerabilities and prepare for changes (Barker et al., 2021). To add an additional layer of security, hybrid cryptosystems are recommended, implemented with proven systems like RSA in case a post-Quantum algorithm were broken (Bindel et al., 2017; Crockett et al., 2019). Furthermore, as development timelines of quantum computers are still elusive and more tangible technological advancements like AI are currently attracting attention and resources

(evolutionQ Inc., 2024), regulatory pressure is needed to accelerate quantum cybersecurity efforts. In a survey conducted by KPMG (2023) on their North American client base, only 25% were addressing the quantum threat within risk management, and all entities surveyed expected longer transition periods than necessary to ensure data confidentiality, while only 11% believed they could become quantum-safe.

Organizations storing time-sensitive data are vulnerable to the quantum threat today. So-called "store now, decrypt later" schemes involve cyber criminals intercepting encrypted information and storing it for decryption once cryptographically relevant quantum computers (CRQC) become available. Mosca's theorem (Mosca, 2015) provides a simple formula to assess the risk exposure of sensitive data:

X = number of years data needs to remain secure
Y = number of years required to migrate to quantum-resistant cryptography
Z = number of years until quantum computers can break currently used cryptography
If $X + Y > Z$, said data is already at risk of being compromised.

The variable Z is commonly referred to as "Q-Day" (Learner et al., 2023), and experts predict that the achievement of a CRQC will happen within a decade (NIST, 2024c). As high levels of uncertainty surround the timeline of this technology, given unpredictable breakthrough-related accelerations and ambiguity around global political agendas (World Economic Forum, 2022), immediate measures should be taken to prepare for the emerging quantum cyber threat landscape.

2.4. Related management concepts

The following summary of key concepts in innovation and dynamic capabilities provides a foundation for understanding how organizations navigate technological change and build resilience against external disruptions.

2.4.1. The Diffusion of Innovation and Technology Acceptance Model

Rogers (1971) introduced the Diffusion of Innovation model, which describes the process in which an innovation spreads over time within a social system. The pace of diffusion is influenced by several attributes such as relative advantage, compatibility, complexity, trialability, and observability. The categories of adopting individuals differ and change

throughout the different stages, with “innovators” and “early adopters” composing the initial groups that are characterized with a higher aptitude for risk and novelty, as opposed to the “late majority” and “laggards” which are rather driven by necessity or external pressure. Understanding these dynamics is crucial for effective introduction and scaling of innovations. Kristensson et al. (2020) expand upon this stating that modern innovations involve continuous, dynamic interactions instead of singular adoption events.

Building on Rogers’ work, Davis shifts focus from objective traits of innovations to the subjective psychological dimensions of users. The Technology Acceptance Model (TAM) describes two main factors influencing the acceptance and use of new technology: Perceived Usefulness (PU), which refers to the extent to which a user expects a technology to enhance job performance; and Perceived Ease of Use (PEOU), which relates to the degree adoption is expected to be free from effort. This model suggests that interplay between these two factors influences user attitudes towards the innovation and ultimately the decision about adoption (Davis, 1987).

2.4.2. Dynamic Capabilities

To address how firms compete in rapidly changing environments, David Teece introduced the concept of Dynamic Capabilities defined as a “firm’s ability to integrate, build, and reconfigure internal and external competences” (Teece et al., 1997). There are three components to dynamic capabilities: processes, or the organizational routines and methods; positions, which are the specific assets impacting the competitive stance; and paths, the strategic direction based on historical decisions. It is important to emphasize the last component, as path dependencies of past decisions make a firm’s competitive trajectory difficult to replicate.

Barreto refined the concept, defining dynamic capabilities as “the firm’s potential to systematically solve problems, formed by its propensity to sense opportunities and threats, to make timely and market-oriented decisions, and to change its resource base” (Barreto, 2010). This perspective operationalizes dynamic capabilities and demonstrates how firms can achieve superior performance by effectively managing change. In practice, this means organizations must gather and process information effectively, act at the optimal time to seize opportunities and mitigate threats, align strategies with the evolution of market demands, and continuously reconfigure their resources to adapt to novel challenges.

Cuthbertson & Furseth (2022) expand on the service perspective by distinguishing between operand (such as raw materials and data) and operant resources (like algorithms and processes). In digital environments, operand resources require frequent updates to remain competitive, while operant resources enable continual innovation and renewal. Unlike traditional resource-based strategies that consider valuable, rare, inimitable, and non-substitutable (VRIN) attributes, digital competitiveness relies on the pace and continuity of innovation.

Complementing dynamic capabilities, O'Reilly and Tushman (2008) introduced organizational ambidexterity, which describes the ability to balance exploration of new opportunities with exploitation of existing capabilities. This dual focus allows firms to innovate and adapt while maintaining operational efficiency and performance, a critical capability to thrive in environments characterized by rapid change and uncertainty.

Unpredictable events, known as exogenous shocks, illustrate the impact of dramatic disruptions in the external environment in which organizations operate. They may stem from technological breakthroughs, political instability, economic downturns, demographic changes, health crises or environmental changes (Teece, 2007), introducing both new risks and opportunities and frequently leading to substantial shifts in firm performance relative to peers. Consequently, firms must align internal resources and strategies with external conditions (Aldrich, 1979; Levinthal, 1991).

3. Methodology

3.1. Research Design

This dissertation analyzes factors influencing the enterprise adoption of post-quantum cryptography. The figure below details the methodology.

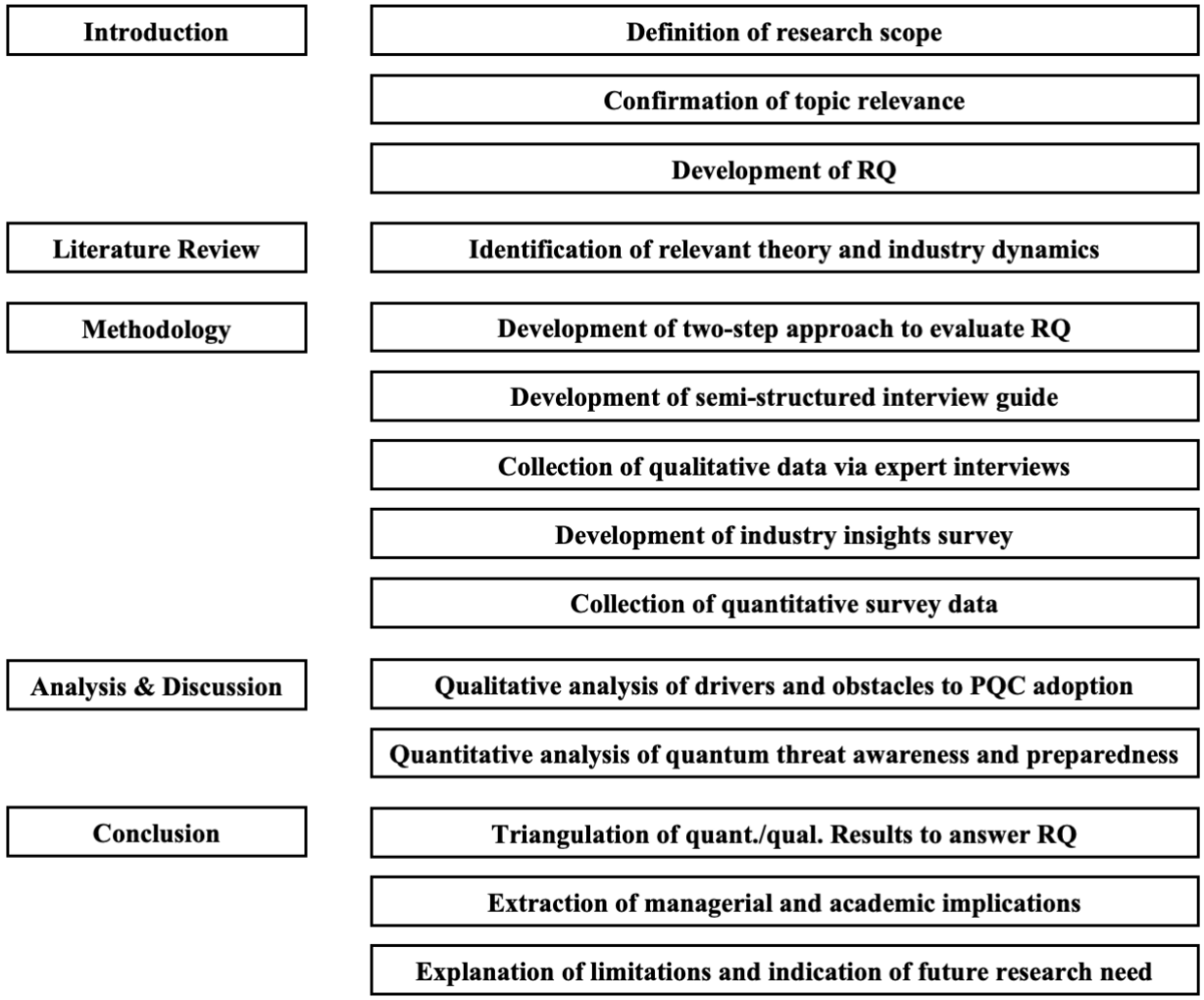

Figure 3: Research Design

A mixed-method approach was employed, combining qualitative interviews and a quantitative survey with inductive as well as deductive methods (Qu & Dumay, 2011; Sekaran & Bougie, 2009; Mayring, 2000). Industry experts from the fields of quantum computing, cryptography and cybersecurity contributed insights in semi structured interviews related to the range of topics covered in the literature review. Based on the findings on adoption factors, a survey on the awareness and preparedness regarding the quantum threat was conducted on Cybersecurity professionals across different industries to validate the expert insights and triangulate with the literature review (Denzin, 2017).

3.2. Data Collection

3.2.1. Primary Data – Expert Interviews

Semi-structured interviews are an accepted method in qualitative business research , which enables the exploration of experiences, beliefs, attitudes and motivations (Barriball & While, 1994; Rowley, 2012) and provides flexibility to adapt the conversation to each expert's specialized knowledge as it unfolds (Magaldi & Berler, 2020). It aids the researcher in comprehending relationships between variables, allows for the registration of non-verbal cues and deeper elaboration on responses, whilst eliminating the need to repeat interviews (Saunders et al., 2019, Cohen & Crabtree, 2006). To guide the interviews with a consistent framework and generate comparable qualitative data, questions were formulated based on prior knowledge (Rowley, 2012).

The script included 6 questions tailored to each interviewee's specific expertise, narrowing focus when an expert had specific domain expertise. There were 88 potential candidates scouted from publications, whitepaper contributions, organizational affiliations and network referrals and were contacted via e-mail, LinkedIn or private channels.
Table 1: Expert profiles lists and details relevant expertise of the 14 anonymized experts who agreed to be interviewed, which allowed us to reach data adequacy and see evidence of data saturation, typically held to require a minimum of twelve experts (Guest et al., 2006). Experts with a broader perspective are classified as "G" for generalists, whilst candidates specialized in cybersecurity, quantum computing and QKD are prefixed with "S".

Interviews were conducted and recorded via Microsoft Teams and lasted an average duration of approximately 30 minutes, whilst being transcribed verbatim for analysis. To identify patterns and trends, a combination of open coding and thematic analysis was used in the process (Krippendorff, 2004). The interview guide and responses are summarized in Appendix A.

Code	Current position and expertise
G1	Venture Capitalist with 5 years of experience developing quantum computers, who actively receives first-hand information from big tech quantum project leads
G2	Senior Manager at a leading multinational management consultancy with over 10 years of experience in cybersecurity and a PhD in experimental physics
G3	Mathematician and NIST fellow, with 30 years of cryptographic research experience and involvement in the standardization of post-quantum cryptographic algorithms
G4	Member of WEF Global Futures Council for Quantum and IEEE Quantum steering committee, as well as representative of Quantum Computing ecosystem in India
G5	Consultant at a leading multinational management consultancy, specialized on cryptography with related post-doctoral research experience
G6	Applied mathematical engineer with 15 years of cryptography experience, leading security architecture at an IoT quantum cybersecurity company
G7	Side Channel Attack (SCA) analyst at a leading quantum cybersecurity company, improving the implementation of algorithms standardized by NIST
G8	Expert on Public Key Infrastructure (PKI) with over 30 years of experience, heading strategy at a PKI-as-a-service company on PQC migration of its products
G9	Cybersecurity consultant with over 15 year of experience and a PhD in cryptology, specialized on national digital security and critical infrastructure
S1	Quantum Application Engineer at a leading quantum computing developer, with expertise in quantum algorithms and a PhD in Quantum Information Theory
S2	Author, advisor and keynote speaker on quantum computing & AI, with over 40 years of IT experience and a PhD in mathematics
S3	Management Consultant on quantum computing applications at a leading quantum computing developer
S4	Global cybersecurity adviser and speaker with experience heading cyber operations in multinational technology and financial service enterprises, as well as the NSA
S5	Sales VP at a leading Quantum Key Distribution (QKD) company with over 12 years of experience on the quantum threat topic

Table 1: Expert profiles

3.2.2. Primary Data – Industry Insights Survey

The literature review and expert interviews established the potential cyber threat imposed by a CRQC, deriving urgency for organizations to assess their cryptographic inventories and invest into crypto agility. A survey directed at cybersecurity professionals was conducted to better

understand levels of awareness and preparedness within enterprises and distributed through direct LinkedIn and E-mail outreaches. Around 1,200 candidates were screened based on position, industry affiliation and geography to ensure a balanced representation. While the financial sector outweighed the others by a factor of 3 due to its significance to this topic and availability of profiles, about 100 profiles of each industry category option in the survey's screening question were listed. Due to privacy settings, roughly 2/3 could be directly contacted, to which approximately 500 direct e-mails and 300 LinkedIn connection requests were distributed.

The survey consisted of 24 questions categorized into 5 sections: Screening questions, awareness & perception of quantum threats, current encryption practices & quantum readiness, risk exposure & management, and adoption factors. The outline of survey questions is listed in Table 5 Outline of survey questions of Appendix B. The Qualtrics platform was used to design and administer the survey in English and without interference by the researcher. Participants were sampled with qualifying questions testing respondents' attention to eliminate invalid responses. In total, 43 respondents started the survey, of which 40 completed all questions and 3 were eliminated by failing to answer the qualifying questions. Hence, only n = 37 valid responses could be collected, sufficient to distinguish initial trends yet unfortunately significantly below the threshold of data representativeness. A minimum sample size of 200 would have been considered representative for populations larger than 10.000 in order to obtain high confidence levels on derived insights. (Krejcie & Morgan, 1970). The data collected was examined using descriptive methods and linear regressions. Likert scales were selected as the most suited approach to effectively capture attitudes (Likert, 1932), which can be treated as interval data for parametric analysis if consistent and evenly spaced (Labovitz, 1970; Traylor, 1983).

3.2.3. Secondary Data

Secondary data was primarily collected during the literature review, which included academic articles, books and reports from science and management journals, as well as reports from consulting firms, governing and standardizing institutions.

4. Results

4.1. Semi-structured interviews

The findings from the interviews are grouped into three main themes in accordance with Mayring's (2000) qualitative content analysis methodology: The state of the art in quantum computing development and its potential applications beyond decryption, the level of awareness on and preparedness for emerging cyber risks like quantum computing, and finally the drivers and obstacles for the adoption of quantum-safe encryption, its technical implementation challenges and future projection.

4.1.1. State of development of quantum computers

The consensus between current expert opinions was that while quantum computing research is progressing, significant technical challenges are yet to be overcome to achieve a fully scalable CRQC. S1 described three layers to measure maturity of this technology: *Quantum utility* demonstrates that a quantum computer can solve a useful, yet not commercially viable problem, mainly for research purposes. With *quantum advantage*, problems with real world commercial applications like drug discovery and optimization can be solved. Finally, *quantum supremacy* describes the outperformance of classical computing. While Google has technically achieved quantum supremacy in 2019 (Arute et al., 2019) and reiterated on this in their 2024 announcement (Google, 2024) that sparked headlines and stock market speculation, the misleading nature of this claim has been viewed critically by most experts. G1, S2 and S3 clarified that the underlying computation was essentially a random sampling experiment with no useful application, in which a large array of random numbers was simulated. While very computationally expensive for a supercomputer, the inherently random nature of qubits simply requires a read-out on a quantum computer. Hence, instead of simulating a quantum circuit, it was essentially sampled, without any relevance to computational speed-up. Expert S3 challenged the supremacy claim in general, as quantum computers will fundamentally serve more specialized use cases than classical computers. According to S1 and S3, quantum utility has already been demonstrated, while quantum advantage being the next milestone that will elevate the industry out of the research phase into commercialization.

The root obstacle to developmental progress is the inherently unstable nature of qubits which interact with the environment, leading to the decay of stored information and errors. As G1,

S1, S2 and S3 pointed out that more important than the number of qubits contained on a computing platform is their ability to integrally network with one another at scale while maintaining their quantum state. Performance benchmarks include fidelity, which measures resistance to errors states, while coherence time describes the number of possible computations before data disintegration. Different quantum computing platforms possess unique performance trade-offs. For example, trapped ions perform well on fidelity and coherence, yet computations are slow, and they are challenging to scale. In contrast, superconducting qubits perform fast computations and are easier to scale yet have poor fidelity and coherence, vastly limiting the number of operations. One approach on improving fidelity is the bundling of multiple physical qubits to average their output and form a logical, error-correcting qubit, as has been outlined by Wang (2012). However, G1 and S2 criticized that ratios for logical qubits are loosely defined and hence obscure the number of physical qubits as a measure for technical progress, as relied on in the literature. S1 that while superconducting qubits are currently the dominant platform, due to established semiconductor manufacturing capabilities that reduce cost and R&D efforts, breakthroughs in other technologies like trapped ions, photonics or neutral atoms can emerge a new leading platform. S2 and S3 claimed that the future of quantum computing will involve a mix of different platforms, each catered to specific use cases based on unique performance requirements and expendable time and resources.

Investments into this technology have been primarily driven by government funds, considering its dual-purpose for national security applications, as mentioned by G4, as well as the uncertain maturity timeline requiring patient capital. Among the few experts that didn't refrain from making timeline predictions, the number of years ranged from 3 to 30 years, exemplifying the ambiguity around developmental progress. G2 noted that current data is insufficiently reliable to make accurate projections and G1 and S2 warned against hype generated by financially incentivized vendors. G1 further elaborated on the issue of a lacking market incentive to drive development by customer funding instead of government funding, as linear grant models perpetuate the academic practice of narrowing conditions to avoid errors and preserve regular funding. On the other hand, G2 and G4 raised awareness on the fallacy of linear thinking and historical underestimations of technological evolution timelines. G6, S3 and S4 added to this sentiment that geopolitical obscurity around this technology may conceal real progress.

4.1.2. Commercial applications of quantum computers

According to S1, S2, S3 and the literature, the main commercial applications for quantum computing will be in optimization problems like in finance or large-scale logistics, in which small efficiency gains can translate to a multiplicative effect on value, as well as simulations of physical processes like molecular interactions for drug or battery development (Mind Commerce, 2020). On the flipside, G1 claimed such applications to be smoke screens for the main application of decryption, with most revenue being sourced from governments or their proxies. S2 called out companies claiming use cases for 2-digit numbers of qubits, illustrating the example of 160 perfect logical qubits being required to simulate just a single caffeine molecule. For viable commercial use, the required number of qubits will be at a similar magnitude as necessary for running Shor's algorithm. According to S1 and S3 who are employed by quantum computing (QC) companies, the technology is not yet capable of providing tangible competitive advantages for real world applications, with the lack of perceived usefulness contributing to the current slow pace of diffusion (Davis, 1987; Kristensson et al., 2020). Hence, clients are mainly contracting cloud access to hardware for exploration and training purposes, while postponing hardware investments until the technology matures. Furthermore, sovereignty issues around this technology limit hardware sales mainly to public institutions in selected countries, explaining universities to be common first adopters (Lewis & Wood, 2023).

4.1.3. Awareness and preparedness for emerging cyber risks like quantum computing

Experts G1, G2, G6 and S4 agreed that cybersecurity risks are typically managed based on urgency, only being prioritized if immediate and quantifiable. G2 and S4 elaborated on how risk assessments factor likelihood and impact, upon which annual budgets are allocated to depending on prioritization for mitigative action. However, G2 and S4 stressed the difficulty in quantifying the risk of quantum computing due to its enormous impact and unknown timing, providing the literature a prime example to confirm the complexity of cyber risk management (Zeller & Scherer, 2022). While PQC is not a big topic within risk management, G5 stated that cryptography is usually considered in compliance assessments, specifically regarding key management practices.

Table 2 below ranks PQC sector awareness by frequency of expert mentions:

Sector	Mentioning experts
Financial Services	G1, G2, G3, G4, G6, G8, S5
Government	G2, G4, G6, G8, S5
Telecommunications	G2, G8
Automotive	G5, G6
Infrastructure	G4
Healthcare & Pharmaceuticals	G4
Big Tech	G3

Table 2: PQC sector awareness

Since the US government mandated the implementation of PQC for all its vendors and the NIST published the first set of algorithm standards (NIST, 2024c), awareness especially among the government and highly regulated financial sector has been increasing (G6, G8), with some organizations starting to allocate funds for initial exposure assessments and studies (S4). However, G8, G9 and S5 agreed that awareness in most organizations is generally still low due to the lack of urgency compared to more imminent cyber threats. The SNDL threat of future decryption is mainly a concern to national security data with long shelf life, with potential implications for corporate IP and trade secrets as well (G1, G4). G6 also mentioned security risks posed by embedded IoT hardware deployed for 10-20 years in vehicles for example, necessitating design considerations for future cryptographic updates. As the literature suggests IoT devices to double in numbers by 2033 (Statista, 2024), their impact will grow in significance.

Beyond focusing solely on the quantum threat however, G9 urged the prioritization of strong foundations in cryptography management, alleviating future algorithm migrations when necessary. G4, G5, S2 and S5 echoed this sentiment by warning about the potential emergence of more efficient factorization methods that could break the NIST standards even with a classical computer, enhanced for example by artificial intelligence. G5 reminded that of the four initially drafted standards in 2023, one was removed after being broken by a classical computer. Hence, as the standardization process of secure encryption schemes is an ever-moving target, it is paramount to transition to a cryptographically agile environment and build cyber resilience (Björck et al., 2015), in alignment with the literature and a fitting example for a dynamic capability. To mitigate the threat of unexpected quantum computing advancements in a rapidly changing environment, cryptographic resources require continuous reconfigurations (Teece et al., 1997). G6 also mentioned hybrid solutions, as detailed in the

literature, in which post-quantum schemes are layered on top of classic ones. However, the only method that can truly guarantee information security is QKD, which eliminates mathematics from the process. Being affiliated with a leading QKD vendor, S5 elaborated on how this technology is typically deployed as a secure network backbone, complemented by PQC in end-to-end devices. By leveraging quantum mechanics to process data, any interception would disrupt the quantum state and lead to immediate detection. Unfortunately, the complexity in requiring physically connected quantum channels makes cost a limiting factor to this technology's use cases, validating the literature (Fedorov et al., 2018).

4.1.4. Drivers and obstacles for the adoption of quantum-safe encryption

Table 3 below ranks drivers for the adoption of PQC by frequency of expert mentions:

Drivers	**Mentioning experts**
Regulations (including anticipation)	G2, G3, G5, G6, G7, G8, G9, S4
Risk (reputational)	G5

Table 3: Drivers for PQC adoption

Most experts clearly agreed on regulations being the main driver for adoption. As the US government has mandated quantum-safety for all federal agencies in the Quantum Computing Cybersecurity Preparedness Act, the entire government serving market will be required to comply to the new NIST standards (Moody et al., 2024). While the financial services industry is not yet official mandated to adopt PQC, G2 claimed that some institutions are anticipating upcoming regulations and allocating budgets to take initial action. Furthermore, G8 and G9 explained how directives like DORA for the financial sector imply cryptographic updates by mandating the setup of appropriate systems to manage cyber risks. Meanwhile, S4 warned against cybersecurity by compliance, which is a common practice according to the literature (White & Caralli, n.d.), as risk management should be approached proactively instead of reactively. Finally, G5 mentioned reputational risk as a secondary driver, with the example of the automotive industry preserving product safety and integrity.

Table 4 below ranks obstacles to the adoption of PQC by frequency of expert mentions:

Obstacles	**Mentioning experts**
Complexity (cost, resources)	G1, G2, G3, G4, G5, G8, G9
Know-how (talent shortage, standards)	G8

Table 4: Obstacles for PQC adoption

The consensus on obstacles to adoption has narrowed down to the complexity of implementing PQC, as detailed in the subsequent paragraph. Associated resource expenditures without tangible returns on investment (G3) prove difficult to secure budgets for, as according to the literature applies to cybersecurity in general (Ashby et al., 2018; Pooser et al., 2018). Furthermore, G8 mentioned knowledge gaps in terms of talent shortages and lacking implementation standards as a secondary obstacle.

4.1.5. Technical challenges in implementing post-quantum cryptography

Big technology companies like Meta, Google and Apple have demonstrated how migration to PQC can be achieved in a relatively short time frame when the entire cryptographic stack is under internal ownership (G1, G2, G3, G7). Challenges arise within enterprises with supply chain dependencies through interoperability with third-party software and cloud infrastructure, which necessitate reliance on external vendors while amplifying complexity and organizational inertia (G2, G5, G8). As shown in the literature, these system integrations have simultaneously been targets for large-scale cyber-attacks (Eling & Schnell, 2020), elevating the importance of robust implementations. G5 added that standards like TLS require centralized migration, and G8 noted that dated applications are no longer even supported in some cases. G1, G4, G5 and G9 agreed on the discovery exercise of assessing the entire software inventory for necessary changes to be the most demanding task, typically involving consulting projects. While initial cryptographic assessment tools are being rolled out, particularly for communication applications, G5 stated that many embedded systems like hardware encryptions can't be scanned. In fact, legacy soft- and hardware prove to be the main reason for long migration timelines due to compatibility issues. In addition to the migration of RSA to ECC from the literature (Joseph et al., 2022), G7 raised the example of pre-1990s cryptography still being supported in modern banking applications. G5 and G8 further specify the symmetric algorithm DES having been classified as unsafe 30 years ago, as well the hash function SHA1 since 2015 which is still being supported by TLS with a planned phase-out in 2030. The performance impacts of the NIST PQC standards on legacy hardware indicate a similar lengthy adoption timeline, with G3 claiming 15, and G8 up to 30 years for complete migration. Implementation experts G6 and G7 claimed bandwidth and memory requirement increases by a factor of 5-10 due to larger key and ciphertext sizes in lattice algorithms. Furthermore, hybrid cryptography and comprehensive protections against

physical side-channel-attacks necessitate additional compute by a factor of up to 5-6. While the experts were aligned concerning the need for a thorough infrastructure upgrade (G2-G7), some pointed towards available interim solutions like software patches and function wrappers (G3, G4), as well as the option to disconnect vulnerable devices from the system (G5-G7). In general, G7 asserted that encryption hardware is more critical for timely migration than devices used for authentication, considering the SNDL threat.

4.1.6. Projections on the adoption of post-quantum cryptography

The publication of NIST standards has generated momentum and increased demand for consulting projects on PQC and cryptographic agility, as well as support built into software libraries and products (G5, G6, G9, S4), including communication standards like IP (internet protocol) and 6G (G3, G8). First movers will include entities processing sensitive information, primarily in the financial services, government and telecommunications sectors (G1, G6, G8). However, adoption rates are generally still low and limited to explorative actions (G1, G5). G2 pointed to the importance of regulations in initiating the process, which would provide learnings that facilitate other industries to follow suit. G1 argued that for adoption to accelerate, a successful hack by a quantum computer is necessary to generate external pressure and highlight the PU (Davis, 1987) of quantum-safe encryption, ultimately compelling late adopters to act.

4.2. Expert survey on the adoption of PQC

The survey results ($n = 37$) are structured in five segments, beginning with a presentation of screening questions and general awareness of the QC Threat. Various responses were aggregated to analyze levels of risk exposure, followed by an overview of mitigative action. Where notable trends were applicable, information on organization size and industry affiliation was considered, whereby critical industries were emphasized in the color scaling. Finally, factors influencing the adoption of PQC were analyzed in a linear regression.

4.2.1. Response Profile

To provide the adequate context for interpretation, a set of screening questions were asked that revealed participants' positions of seniority, industry affiliation, the size of employing organization and location of its headquarters. Figure 4: (Q1) Distribution of Roles shows that nearly 2/3 of responses came from C-Level executives, typically Chief Information Security Officers (CISO), indicating an optimal level of organizational oversight suited for this topic. Technology was the most responsive industry, followed by the critical financial services, government and military sectors (Li and Liu 2021, Kang et al., 2015), as detailed in Figure 5: (Q2) Industry Affiliation The range of industries was limited to those with data security risks requiring the appointment of cybersecurity professionals, as would less likely be the case with retail or fashion for example.

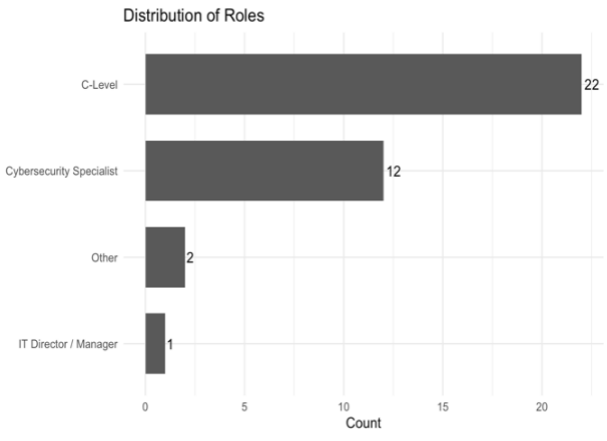

Figure 4: (Q1) Distribution of Roles

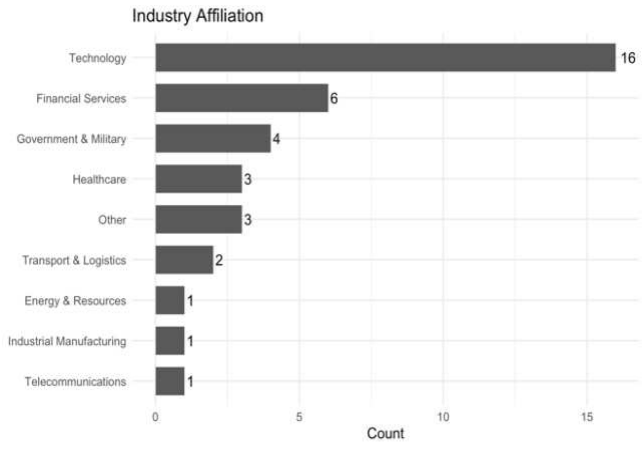

Figure 5: (Q2) Industry Affiliation

Roughly 2/3 were employed by organizations with a headcount above 1,000, with all of the government sector being on the higher range above 10,000. Notably, the financial services organizations were all below 10,000, implying that no major banks were surveyed. Finally,

the locations of organization headquarters are mapped out in Figure 7: (Q4) Organization Headquarters, in which of the 24 included countries, only Brazil (2), Switzerland (4), Germany (5) and the USA (10) had more than one representative and are highlighted accordingly.

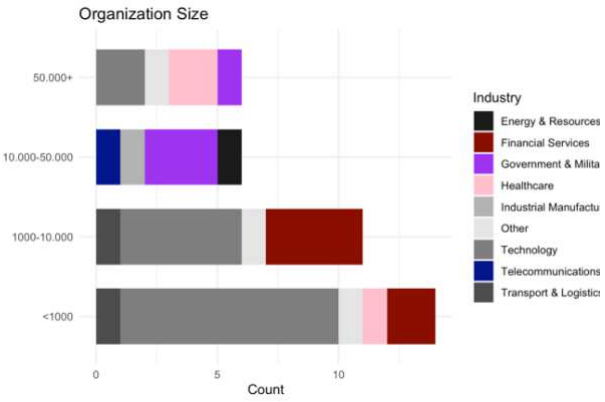

Figure 6: (Q3) Organization Size

Figure 7: (Q4) Organization Headquarters

4.2.2. General awareness of the quantum computing threat

At first, the level of awareness on the cybersecurity threat of a CRQC was assessed and scrutinized next to the SNDL Threat and practice of Cryptoagility. Nine out of 10 respondents claimed to be at least *moderately familiar*, of which 46% were *very familiar* and 16% were domain experts. This indicates topic unfamiliarity as a deterrent that potentially led to the low response rates. In comparison with knowledge on the SNDL Threat, while the number of at least *very familiar* respondents slightly increased, the share of those *slightly familiar* and below rose to 27%. Familiarity on Cryptoagility is overall 10% lower in comparison, revealing a slightly lower level of understanding on the full scope of the topic than specified.

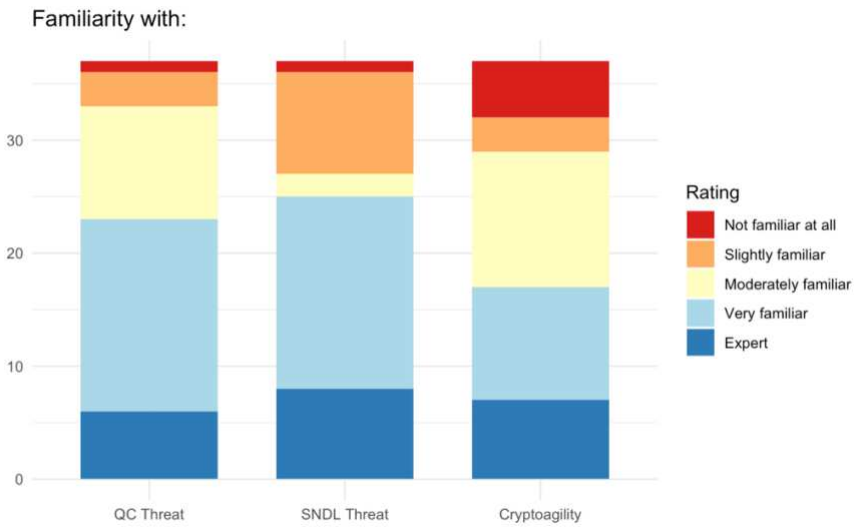

Figure 8: Familiarity with the QC (Q5) & SNDL (Q6) Threats and the practice of Cryptoagility (Q7)

When broken down by industry and organization size, Figure 9 shows that larger organizations and critical sectors like Government & Military are generally more aware of the QC Threat, which aligns with findings from the literature (Moody et al., 2024) and expert interviews (Table 2). This trend is reflected in Figure 10 on the actual concern about the threat, despite an overall balanced distribution around the moderate sentiment. It is worth noting that while the globally regulated financial industry (S4) is not as concerned, the responses from this dataset do not represent major financial institutions.

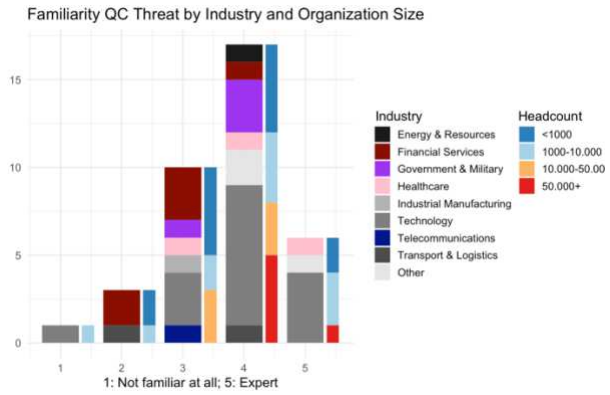

Figure 9: (Q5) Familiarity of QC Threat by Industry and Organization Size

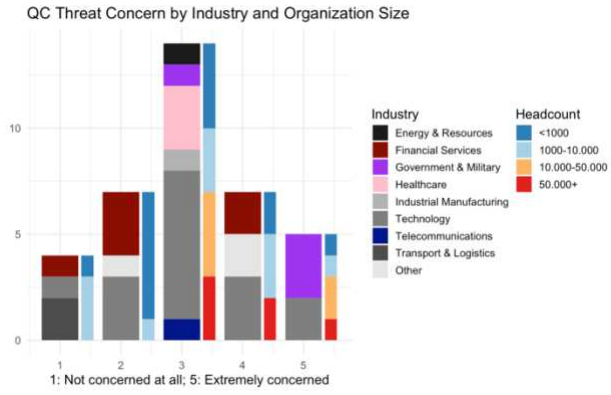

Figure 10: (Q8) QC Threat Concern by Industry and Organization Size

4.2.3. Risk exposure to the QC Threat

The level of risk exposure to the QC Threat was evaluated by comparing responses related to cryptography management, encryption usage, data sensitivity and PQC migration timelines.

Overall, most organizations had a good overview on the cryptographic inventory, with 70% specifying that they had at least a *moderate level* of assessment completed. Notably, half of large organizations above a headcount of 10.000 have achieved a *high level* of assessment despite the elevated complexity commonly associated with size (Table 4). Figure 12 reveals the asymmetrical encryption schemes used throughout different industries. Evidently, the widely adopted RSA standard was most used by a factor of 1.6 in comparison to its upgrade, ECC, as expected from the literature on the inertia of adopting new standards (Joseph et al., 2022). While 11% have already implemented the NIST standard ML-KEM, 32% were still using the vulnerable precursor to RSA, DH (Diffie & Hellman, 1976). It is also alarming that amongst those who answered *Uncertain*, nearly all belonged to critical industries.

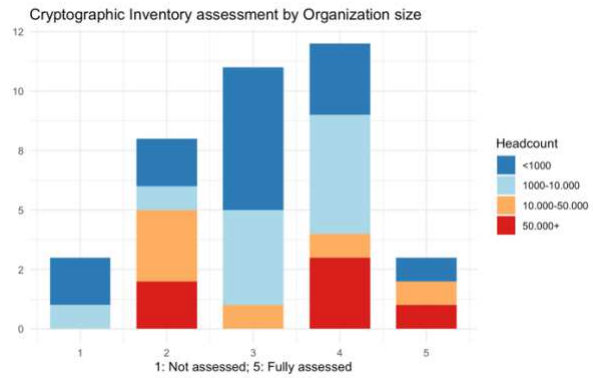

Figure 11: (Q10) Cryptographic Inventory assessment by Organization size

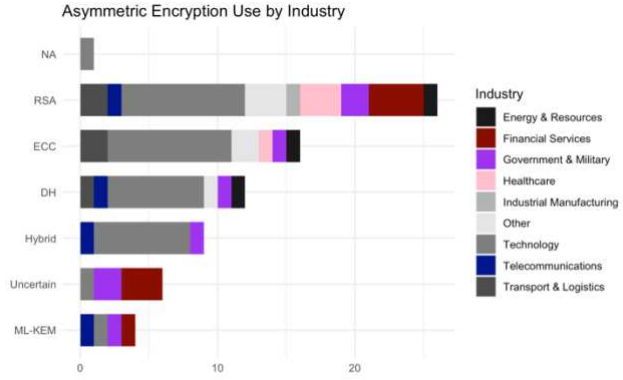

Figure 12: (Q11) Asymmetric Encryption Use by Industry

For the migration to PQC, critical industries were more dependent on third-party vendors than the average, as displayed in Figure 13. Many less-dependent organizations were in the Technology industry, which are more likely to own their cryptographic stack and have internal technical capabilities (Barker et al., 2021), exemplifying the advantage of dynamic capabilities in mitigating threats and adapting to change (Barreto, 2010). Overall, nearly 90% of organizations were at least *slightly dependent*, and 2/3 relied on external vendors for key management, underscoring the scope and complexity associated.

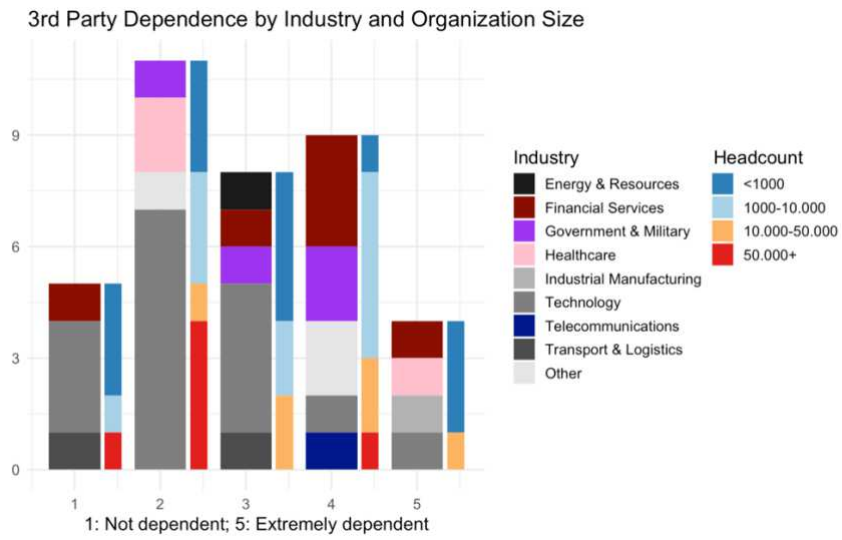

Figure 13: (Q23) 3rd Party Dependence by Industry and Organization Size

A series of questions were asked to address implications related to the SNDL Threat. On the confidentiality timeline of processed data, 35% specified a period of 15+ years, of which critical industries comprised half the population. The obligation of Government & Military sectors to safeguard state secrets aligns with this trend. For more than half of respondents, data was required to remain confidential only up to 10 years. Furthermore, 53% estimated the transition period to PQC to take only up to 5 years, with 86% expected to have completed the process in 10. While the literature referred to extensive migration timelines across industries spanning decades (Barker et al., 2021), these results revealed that individual organizations can take significantly less time to upgrade their cryptography. Hence, it is potentially the cumulation of legacy systems and devices that primarily elongates standards updates.

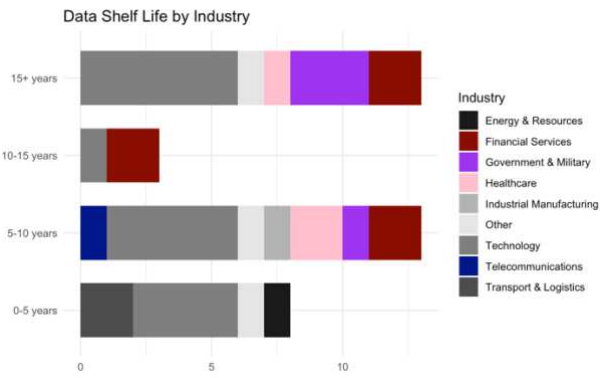

Figure 14: (Q17) Data Shelf Life by Industry

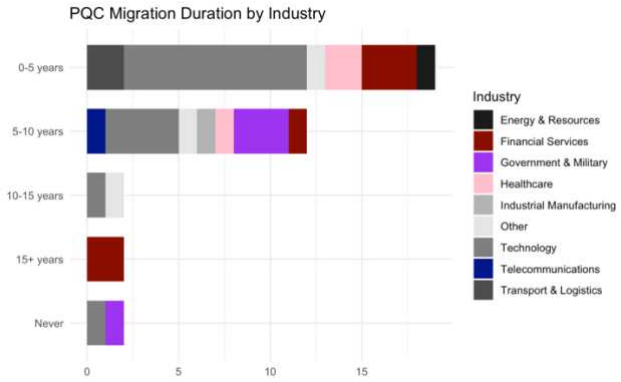

Figure 15: (Q19) PQC Migration Duration by Industry

According to Figure 16, 95% of respondents expected a CRQC to be available within 15 years, with over 1/3 of the population estimating as soon as up to 5 years, showcasing uncertainty around the technological development timeline as expressed in the expert

interviews. We saw that 30% have already begun transitioning to PQC, while 40% plan to start within 0-5 years, including the Government & Military sectors in alignment with their data security obligations. Relating to Mosca's theorem (Mosca, 2015), the risk assessment of the distinguishable single Telecommunications respondent can be backtracked as an example, based on the available data. The data shelf life (X) of 5-10 years and expected equal migration duration (Y) sum up to 10-20 years. With an expected CRQC available (Z) in 10-15 years, in the optimistic scenario ($X + Y = 10$ years; $Z = 15$ years), up to 5 years remain to begin transition before $X + Y > Z$ and data is at risk of being compromised. As migration was planned within 0-5 years, the optimistic scenario was relied on in this instance.

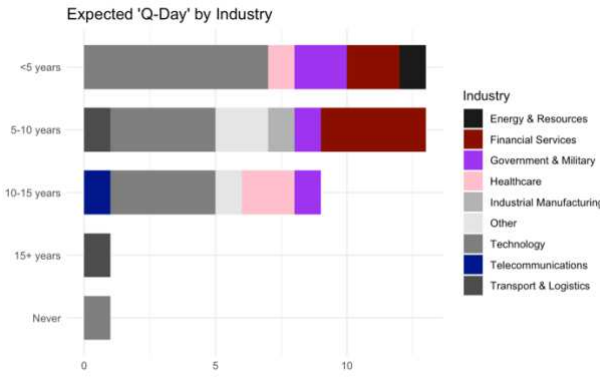

Figure 16: (Q9) Expected 'Q-Day' by Industry

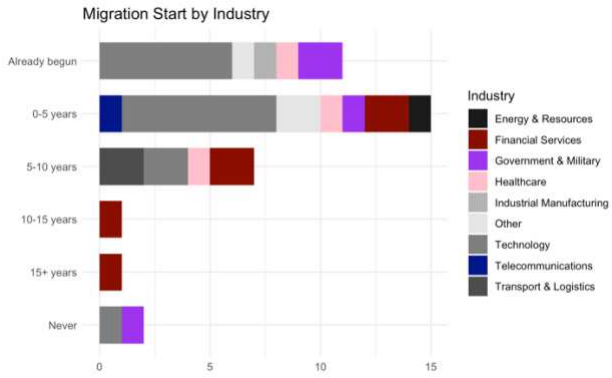

Figure 17: (Q18) Migration Start by Industry

Beyond the decryption of sensitive information, another major risk is the operational disruption caused by classic cyber-attacks like Malware and Denial of Service (ENISA, 2024), in this case facilitated by a QC. According to survey findings, 95% of respondents acknowledged potential exposure, with 70% anticipating at least moderate operational disruption, exhibiting the difficulty of quantifying the scale of impact.

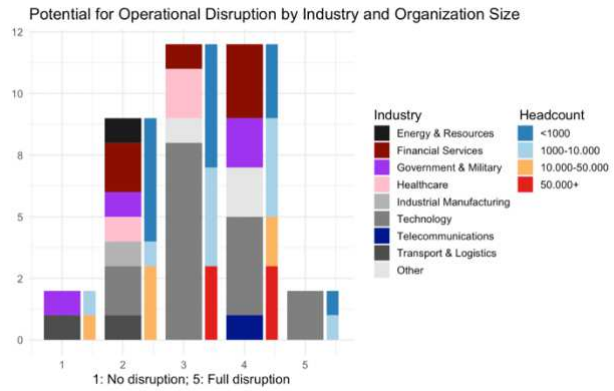

Figure 18: (Q15) Potential for Operational Disruption by Industry and Organization Size

4.2.4. Risk Management

Participants were asked to specify their organization's level of risk exposure to the QC Threat and to what extent it is integrated into the risk management strategy. The results were substantially correlated (0.65) and on average 5% higher on the latter question, inferring proactivity among respondents in addressing the threat according to their risk profile. In contrast to the survey conducted by KPMG (2023), in which only 25% of their North American client base were addressing the quantum threat within risk management, it was addressed by nearly 90% of participants in this study.

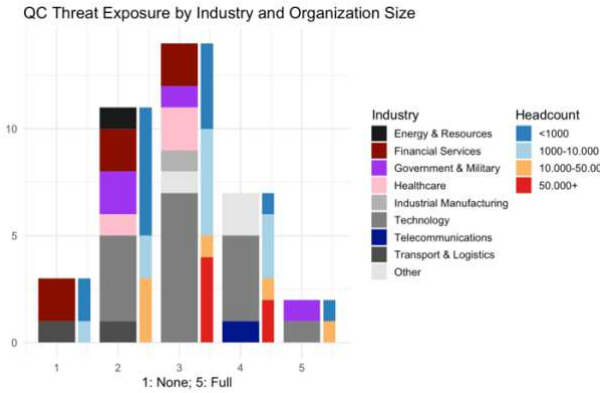

Figure 19: (Q14) QC Threat Exposure by Industry and Organization Size

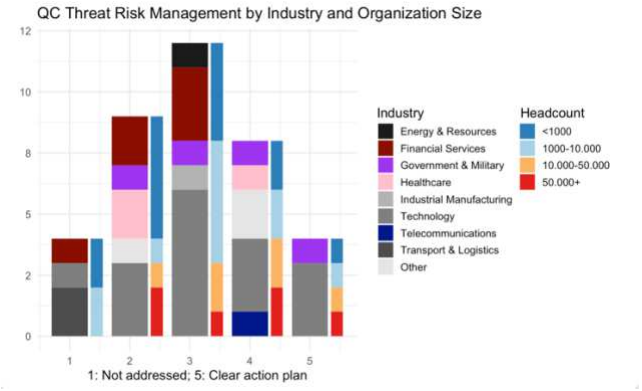

Figure 20: (Q16) QC Threat Risk Management by Industry and Organization Size

Despite high levels of risk consideration, 43% had no budget allocated for the appropriate mitigative action of migrating to PQC (NIST, 2024c). Merely 14% had sufficient funds for implementation, validating the literature on overall negligence of cybersecurity threats until they are quantifiable and immediate (Ashby et al., 2018; Pooser et al., 2018). 1/5 planned to wait for regulations before migrating, whilst 30% already started and 27% are planning to start regardless, relativizing the impact of this factor on adoption.

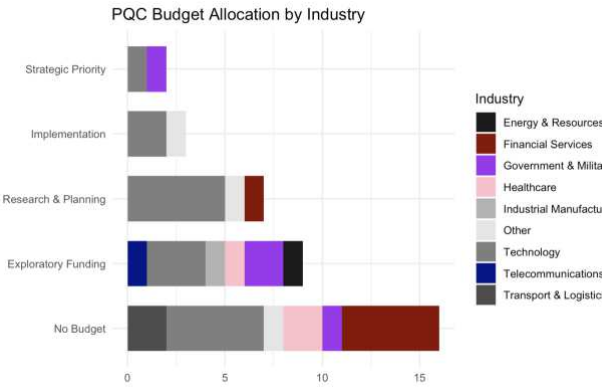

Figure 21: (Q20) PQC Budget Allocation by Industry

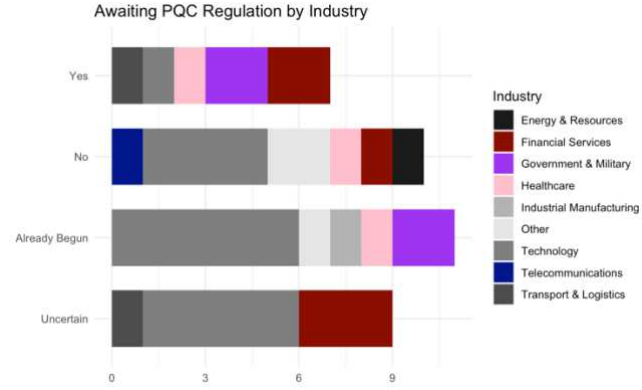

Figure 22: (Q22) Awaiting PQC Regulation by Industry

4.2.5. Adoption factors

Respondents were asked to rate the level of significance of several factors on their level of action for migration to PQC, which were induced from the literature and expert interviews. As detailed in Figure 23, reputation was the most significant, followed by leaps in QC development, and regulations, which can be consolidated as external risks. Budget constraints and the availability of standards were also above the moderate significance level, partially validating findings from the expert interviews (Table 4). Less impactful were talent shortages, process constraints, the availability of third-party vendors, and by the largest margin least impactful, competitor moves.

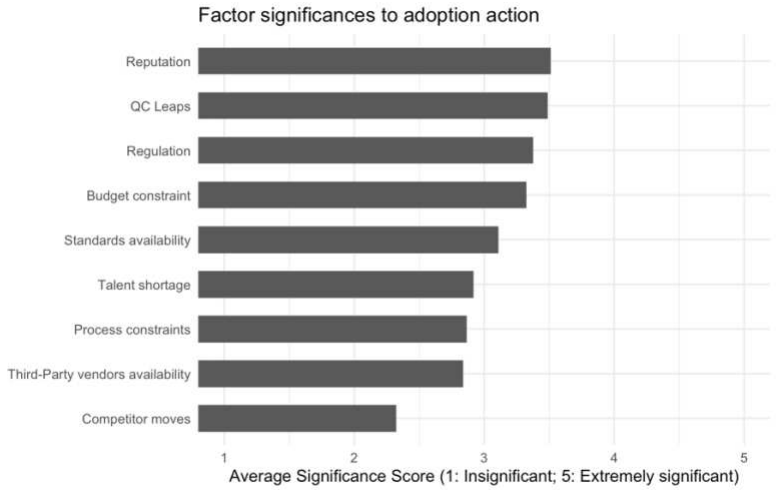

Figure 23: (Q21) Factor significances to adoption decision

A linear regression was performed to examine adoption factors in greater depth, regressing various independent variables with comparable intervals against three dependent variables that indicated action on adoption: Migration Start (Q18), Risk Management (Q16), and PQC Budget Allocation (Q20). To avoid multicollinearity issues, all independent variables were mapped on a correlation matrix. In correlations of above 0.7, the variable with higher Variance Inflation Factor (VIF) value was retained. Notable logical correlations included the level of risk exposure (Q14) with both the potential for operational disruption (Q15) of 0.69, as well as the concern about the QC threat (Q8) of 0.74, as a high level of risk would naturally lead to increased concern. Screening questions on industry affiliation and organization size were excluded due to the large range of values that would significantly compromise a regression on a low sample size. After removing redundancies, the final list of independent variables was narrowed to match the ones identified in the literature and expert interviews,

including each 5 drivers and obstacles in subsequent order. The average VIF value was around 1.5, with none ranging above 2.6, indicating an acceptable level of multicollinearity. The regression output is detailed in Figure 24: Regression output below:

	Dependent variable:		
	(Q18) Migration Start	(Q16) Risk Management	(Q20) PQC Budget
	(1)	(2)	(3)
(Q21) Regulation	-0.129 (0.186)	-0.104 (0.144)	-0.053 (0.139)
(Q21) Reputation	0.160 (0.252)	0.142 (0.196)	-0.136 (0.189)
(Q21) Competitor moves	-0.044 (0.207)	0.126 (0.161)	0.146 (0.155)
(Q9) Decryption Timeline	-0.071 (0.228)	0.122 (0.177)	0.083 (0.171)
(Q14) Exposure	0.656** (0.249)	0.705*** (0.194)	0.879*** (0.187)
(Q21) Budget constraint	0.131 (0.240)	-0.085 (0.186)	-0.003 (0.180)
(Q21) Process constraints	0.095 (0.294)	-0.092 (0.229)	0.088 (0.221)
(Q21) Talent shortage	-0.029 (0.232)	-0.114 (0.180)	-0.105 (0.174)
(Q21) Standards availability	-0.112 (0.218)	-0.050 (0.169)	0.153 (0.163)
(Q23) Supplier Dependency	0.208 (0.195)	0.157 (0.151)	-0.045 (0.146)
Constant	1.277 (1.553)	0.626 (1.206)	-0.704 (1.164)
Observations	37	37	37
R2	0.367	0.527	0.590
Adjusted R2	0.124	0.345	0.433
Residual Std. Error (df = 26)	1.216	0.944	0.912
F Statistic (df = 10; 26)	1.509	2.893**	3.748***
Note:			*p<0.1; **p<0.05; ***p<0.01

Figure 24: Regression output

As expected from the low sample size of $n = 37$ observations, the p values of the regression output were mostly too far above the threshold for statistical significance, resulting in conflicting positive and negative effects across the three related dependent variables. The positive or negative effects of independent variables with aligned aggregated trends can be inferred as the significant outcome. While less conclusive, the dominant trends were chosen from conflicting variables to ensure comprehensive analysis. The low R^2 values further limit the explanatory fit of this model for predictions or generalizations.

The first block of 5 independent variables represented the drivers of adoption which was expected to return positive aggregated coefficients. While applicable in every other case, Regulation (Q21) returned a negative value across all three dependent variables, further relativizing its significance as a primary driver for adoption and challenging expert opinions (Table 3). The results in Figure 22 support this outcome as merely 18% of respondents planned to await regulatory mandates before taking action. The only statistically significant variable was Exposure (Q14), validating the technology acceptance model with higher levels of risk increasing the perceived usefulness (Davis, 1987) and hence the likelihood of

migrating to PQC by a large margin. Reputation (Q21), Competitor moves (Q21) and expected imminence of the Q-Day (Q9) returned similar positive effects, consolidating external risks as primary drivers in alignment with the findings of Figure 23, though less conclusively.

The second block represented the obstacles of adoption and was expected to return negative aggregated coefficients. Two variables returned positive values instead: Process constraints (Q21) and Supplier Dependency (Q23), revealing that these factors were less significant inhibitors that warranted action regardless. In alignment with the literature, a lack of available resources such as Budget (Q21), Talent (Q21) and Standards (Q21) inhibited organizations from taking action on cryptographic updates, reiterating the importance of dynamic capabilities (Teece et al., 1997) and organizational ambidexterity (O'Reilly & Tushman, 2008) in effectively aligning resources and strategies for resilience against exogenous shocks (Teece, 2007), such as the emergence of a CRQC. The ability to balance innovation in operant resources like algorithms (Cuthbertson & Furseth, 2022) while maintaining operational performance ensures both agility and security in an evolving threat landscape.

Finally, an optional open-ended question allowed respondents to comment on additional factors that would alleviate transition to PQC, of which the overwhelming sentiment was the availability of standardized implementation guidelines in the form of libraries, trusted reference implementations, and directives, underscoring the relevance of Standards (Q21) as an obstacle.

5. Conclusion

5.1. Main Findings

This study, based on a triangulation of literature, expert interviews and survey data, finds that while the QC Threat is widely recognized, its impact on the adoption of PQC varies significantly with organization size and across industries. This is something that accords with the literature and our intuitions about organizations. Larger organizations and highly regulated sectors such as government and financial services exhibit greater awareness and proactive measures, while smaller organizations and other industries remain reactive.

The findings confirm that adoption is largely driven by risk exposure, reputational concerns, and regulations. A key departure from prior literature and expert perspectives is that regulatory pressure, while significant, is not the sole driver of adoption. Accelerated by the publication of NIST PQC algorithms (NIST, 2024c), many organizations are initiating PQC migration in anticipation of future threats according to their risk profile, rather than waiting for compliance mandates. The risk of SNDL attacks is particularly concerning for government and financial institutions handling long-shelf-life data, necessitating vulnerability assessments like Mosca's theorem (Mosca, 2015) to evaluate the potential timeframe in which delayed action could result in data compromise.

On the other hand, major obstacles include resource constraints and knowledge gaps in terms of budget, talent, and implementation standards. The most challenging task during the migration process is the cryptographic inventory assessment, which increases in complexity when third-party vendors and system integrations are involved. Among survey participants, 2 out of 3 relied on external vendors for key management and nearly 90% suffered supplier dependencies. While not necessarily an inhibitor for decision-making about migrations, it certainly poses an operational obstacle which effects long migration timelines of several years. Another obstacle is legacy systems, which are a leading cause for delaying discontinuations of obsolete encryption standards. Even among the surveyed population, 32% were still using DH, which exhibits the severity of this problem and suggests a similar trend for adoption of post-quantum algorithms.

Despite these challenges, both expert and survey data suggest that PQC adoption will accelerate as awareness of risk exposure increases and more implementation guidelines become available. The study underscores the need for organizations to move beyond a

compliance-driven approach to cybersecurity and adopt a more strategic, resilient model in response to evolving vulnerabilities and technological advancements requiring increasingly frequent cryptographic overhauls. This includes investments into dynamic capabilities that enable continuous cryptographic assessments and agile key management, allowing for hybrid solutions and swift transitions of encryption schemes as spearheaded by the technology sector.

5.1.1. Theoretical Implications

The findings contribute to existing theories on innovation adoption and dynamic capabilities, offering new insights into how firms respond to emerging cybersecurity threats. This study extends the TAM (Davis, 1987) in the context of cybersecurity applications by demonstrating that perceived levels of risk exposure influenced Perceived Usefulness in adopting mitigative solutions such as PQC.

The study also aligns with the Dynamic Capabilities and Ambidexterity framework (Teece et al., 1997, O'Reilly & Tushman, 2008), emphasizing that organizations capable of effectively aligning resources and strategies to manage and update operant resources (Cuthbertson & Furseth, 2022) such as cryptographic algorithms, whilst maintaining operational continuity, possess a critical advantage in responding to disruptive exogenous shocks such as emerging QC threats (Teece, 2007).

5.1.2. Practical Implications

For industry professionals, the results underscore the urgency of preparing for post-quantum cybersecurity. Organizations should prioritize building cryptographic agility by implementing systematic key assessments, developing transition roadmaps, and leveraging hybrid encryption solutions. Given the unpredictability of CRQC timelines, firms must integrate QC threats into enterprise risk management frameworks to ensure preparedness against unexpected technological leaps.

Policymakers and industry leaders should work together to accelerate the standardization of implementation guidelines. The study highlights the importance of inter-industry collaboration in overcoming knowledge gaps and ensuring seamless cryptographic transitions. Additionally, regulatory bodies should not only incentivize proactive PQC migration through

funding initiatives and compliance frameworks but also advance regulatory measures in parallel to ensure a structured and timely transition.

A key takeaway for cybersecurity professionals is the importance to shift from traditional compliance-driven approaches to a more strategic risk management model. Implementing robust cryptographic governance, training personnel on emerging encryption standards, and fostering a culture of cyber resilience will be essential for organizations navigating the post-quantum era.

5.2. Limitations

This study is subject to several limitations that warrant consideration when interpreting the findings. The reliance on expert interviews and survey responses introduces potential selection biases (Heckman, 1979).

The interview process and structured guide relied on researcher judgement, which may reflect inherent biases. Although participants represented diverse expertise and perspectives, those with professional stakes in the topic area may have contributed biased viewpoints. Additionally, time constraints during interviews necessitated prioritizing certain discussion areas, potentially limiting comprehensive exploration of all relevant topics.

Besides the critical limitation of low sample size, the manual selection process of experts for the survey and voluntary participation may have attracted individuals with stronger topic interest, potentially affecting the generalizability of findings across broader industry contexts. The technology sector is notably represented in the sample, providing valuable insights from this domain yet potentially underrepresenting other industry perspectives. Furthermore, self-reported survey data may include response inconsistencies (Bryman, 2016), and Likert scale measures can induce positive anchoring (Krosnick, 1999). Finally, the application of regression methods on qualitative insights potentially introduces subjective, biased interpretation on data.

5.3. Future Research

Future research should expand on this study by increasing sample size and industry diversity to enhance generalizability across various sectors. Additionally, future studies could focus on longitudinal assessments of PQC adoption to track how firms adapt over time and measure the

effectiveness of different migration strategies. Given the reliance on third-party vendors, further research could investigate supply chain dependencies in cryptographic transitions and how organizations manage external risks. Finally, examining regional regulatory differences and their impact on adoption timelines could offer valuable insights into how compliance landscapes shape cybersecurity decision-making on a global scale. Since regulation is clearly a significant driver, future research could isolate this factor and explore a Research Question concerning how regulation will drive PQC adoption and what forms and features of regulation could accelerate the process.

Bibliography

Acharya, R., Aleiner, I., Allen, R., Andersen, T. I., Ansmann, M., Arute, F., Arya, K., Asfaw, A., Atalaya, J., Babbush, R., Bacon, D., Bardin, J. C., Basso, J., Bengtsson, A., Boixo, S., Bortoli, G., Bourassa, A., Bovaird, J., Brill, L., … Google Quantum AI. (2023). Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, *614*(7949), 676–681. https://doi.org/10.1038/s41586-022-05434-1

Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2018). Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger*, *3*. https://doi.org/10.5195/ledger.2018.127

Ajtai, M., Kumar, R., & Sivakumar, D. (2001). A sieve algorithm for the shortest lattice vector problem. *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, 601–610. https://doi.org/10.1145/380752.380857

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Aldrich, H. (1979). *Organizations and Environments*. Prentice-Hall.

Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), Article 8. https://doi.org/10.3390/app11083678

Allianz. (2024). *Allianz Risk Barometer Identifying the major business risks for 2024*. Corporate. https://www.allianz-trade.com/en_global/news-insights/economic-insights/risk-barometer-2024.html

Alnahawi, N., Schmitt, N., Wiesmaier, A., Heinemann, A., & Grasmeyer, T. (2023). *On the State of Crypto-Agility* (2023/487). Cryptology ePrint Archive. https://eprint.iacr.org/2023/487

Althobaiti, O. S., & Dohler, M. (2020). Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World. *IEEE Access*, *8*, 157356–157381. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3019345

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Ashby, S., Buck, T., Nöth-Zahn, S., & Peisl, T. (2018). Emerging IT Risks: Insights from German Banking. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 180–207. https://doi.org/10.1057/s41288-018-0081-8

Barker, W., Polk, W., & Souppaya, M. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04282021

Barreto, I. (2010). Dynamic Capabilities: A Review of Past Research and an Agenda for the Future. *Journal of Management*, *36*(1), 256–280. https://doi.org/10.1177/0149206309350776

Barriball, K., & While, A. (1994). Collecting data using a semi-structured interview: A discussion paper. *Journal of Advanced Nursing*, *19*(2), 328–335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. https://doi.org/10.1038/nature23461

Bindel, N., Herath, U., McKague, M., & Stebila, D. (2017). Transitioning to a Quantum-Resistant Public Key Infrastructure. In T. Lange & T. Takagi (Eds.), *Post-Quantum Cryptography* (pp. 384–405). Springer International Publishing. https://doi.org/10.1007/978-3-319-59879-6_22

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, *353*, 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

Bravyi, S., Cross, A. W., Gambetta, J. M., Maslov, D., Rall, P., & Yoder, T. J. (2024). *High-threshold and low-overhead fault-tolerant quantum memory* (arXiv:2308.07915). arXiv. https://doi.org/10.48550/arXiv.2308.07915

Bryman, A. (2016). *Social Research Methods* (5th ed.). London: Oxford University Press.

Castelvecchi, D. (2023). IBM releases first-ever 1,000-qubit quantum chip. *Nature*, *624*(7991), 238–238. https://doi.org/10.1038/d41586-023-03854-1

Cebula, J. J., Popeck, M., & Young, L. (2018). *A Taxonomy of Operational Cyber Security Risks Version 2*. 544936 Bytes. https://doi.org/10.1184/R1/6571784.V1

Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity*, *10*(1), tyad023. https://doi.org/10.1093/cybsec/tyad023

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography* (NIST Internal or Interagency Report (NISTIR) 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

CISA. (2021, July 20). *Cyber-Attack Against Ukrainian Critical Infrastructure | CISA*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA, NSA, & NIST. (2023). *Quantum-Readiness: Migration to Post-Quantum Cryptography*.

Cohen, D., & Crabtree, B. (2006). *Qualitative Research Guidelines Project*. Robert Wood Johnson Foundation, Princeton.

Crockett, E., Paquin, C., & Stebila, D. (2019). *Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH* (2019/858). Cryptology ePrint Archive. https://eprint.iacr.org/2019/858

Cuthbertson, R. W., & Furseth, P. I. (2022). Digital services and competitive advantage: Strengthening the links between RBV, KBV, and innovation. *Journal of Business Research*, *152*, 168–176. https://doi.org/10.1016/j.jbusres.2022.07.030

Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, *2023*(10), 1000–1021. https://doi.org/10.1080/03461238.2023.2191869

Davis, F. D. (1987). *User acceptance of information systems: The technology acceptance model (TAM)* [Working Paper]. http://deepblue.lib.umich.edu/handle/2027.42/35547

Denzin, N. K. (2017). *The Research Act: A Theoretical Introduction to Sociological Methods*. Routledge. https://doi.org/10.4324/9781315134543

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. IEEE Transactions on Information Theory. https://doi.org/10.1109/TIT.1976.1055638

Dwivedi, A., Saini, G. K., Musa, U. I., & Kunal. (2023). Cybersecurity and Prevention in the Quantum Era. *2023 2nd International Conference for Innovation in Technology (INOCON)*, 1–6. https://doi.org/10.1109/INOCON57975.2023.10101186

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, *10*(2), 303–333. https://doi.org/10.1007/s13385-020-00250-1

Eling, M., Elvedi, M., & Falco, G. (2023). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

Eling, M., & Schnell, W. (2020). Capital Requirements for Cyber Risk and Cyber Risk Insurance: An Analysis of Solvency II, the U.S. Risk-Based Capital Standards, and the Swiss Solvency Test. *North American Actuarial Journal*, *24*(3), 370–392. https://doi.org/10.1080/10920277.2019.1641416

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

ENISA. (2024). *ENISA Threat Landscape 2024* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

EU. (2024). *Cybersecurity: How the EU tackles cyber threats*. Consilium. https://www.consilium.europa.eu/en/policies/cybersecurity/

evolutionQ Inc. (2024). *Quantum Threat Timeline: Executive Perspectives on Barriers to Action*.

Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. *Nature*, *563*(7732), 465–467. Scopus. https://doi.org/10.1038/d41586-018-07449-z

Fernandez-Carames, T. M. (2020). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), 6457–6480. Scopus. https://doi.org/10.1109/JIOT.2019.2958788

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*(6), 467–488. https://doi.org/10.1007/BF02650179

Fortune Business Insights. (2024a). *Cybersecurity Market Size, Share, Analysis | Global Report 2032* (FBI101165). Fortune Business Insights. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Fortune Business Insights. (2024b). *Quantum Computing Market Size, Value | Growth Analysis [2032]* (FBI104855). https://www.fortunebusinessinsights.com/quantum-computing-market-104855#

GAO. (2021, May 20). *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market | U.S. GAO*. https://www.gao.gov/products/gao-21-477

GDPR.EU. (2018, July 11). *What are the GDPR Fines?* GDPR.Eu. https://gdpr.eu/fines/

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Gilkes, K. (2023). *Preparing for quantum cybersecurity now*. EY. https://www.ey.com/en_gl/insights/innovation/why-organizations-should-prepare-for-quantum-computing-cybersecurity-now

Goldman Sachs. (2019). *Americas Insurance Property & Casualty The cyber market Why insurers saw very limited losses despite large cyber events, and how that could change*.

Google. (2024, December 9). *Meet Willow, our state-of-the-art quantum chip*. Google. https://blog.google/technology/research/google-willow-quantum-chip/

Gouzien, É., & Sangouard, N. (2021). Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory. *Physical Review Letters*, *127*(14), 140503. https://doi.org/10.1103/PhysRevLett.127.140503

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96*, 212–219. https://doi.org/10.1145/237814.237866

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hallenbeck, J. (2024). *Data of 3 billion people exposed in one of the largest data breaches in history*. https://www.yahoo.com/news/data-3-billion-people-exposed-135630094.html

Heckman, J. J. (1979). Sample Selection Bias as a Specification Error. *Econometrica*, *47*(1), 153–161. https://doi.org/10.2307/1912352

Holmes, S., & Chen, L. (2021). *Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies* (2021/967). Cryptology ePrint Archive. https://eprint.iacr.org/2021/967

IBM. (2023). *Charting the course to 100,000 qubits | IBM Quantum Computing Blog*. https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

IBM, & Ponemon. (2018). *Calculating the Cost of a Data Breach in 2018*. https://www.ibm.com/support/pages/calculating-cost-data-breach-2018

IBM, & Ponemon. (2024). *Cost of a data breach 2024 | IBM*. https://www.ibm.com/downloads/cas/1KZ3XE9D

Jogenfors, J. (2019). *Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics*. 245–252. Scopus. https://doi.org/10.1109/BLOC.2019.8751473

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kang, B., Maynard, P., McLaughlin, K., Sezer, S., Andrén, F., Seitl, C., Kupzog, F., & Strasser, T. (2015). Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, 1–8. https://doi.org/10.1109/ETFA.2015.7301457

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b

Koops, B.-J. (2016). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In B. Akhgar & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (pp. 3–15). Springer International Publishing. https://doi.org/10.1007/978-3-319-38930-1_1

Kotas, W. (2000). A Brief History of Cryptography. *Chancellor's Honors Program Projects*. https://trace.tennessee.edu/utk_chanhonoproj/398

KPMG. (2023). *KPMG Market Survey on Cryptography and Quantum Computing*.

KPMG. (2024). *Quantum is coming—And bringing new cybersecurity threats with it*. KPMG. https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607–610.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (Vol. 2). Thousand Oaks, CA: Sage Publications.

Kristensson, P., Pedersen, P. E., & Thorbjørnsen, H. (2020). New perspectives on consumer adoption and diffusion of innovations. *Journal of Business Research*, *116*, 522–525. https://doi.org/10.1016/j.jbusres.2020.04.048

Krosnick, J. A. (1999). *Maximizing measurement quality: Principles of good questionnaire design*. Academic Press.

Kshetri, N. (2018). The Economics of Cyber-Insurance. *IT Professional*, *20*(6), 9–14. IT Professional. https://doi.org/10.1109/MITP.2018.2874210

Labovitz, S. (1970). The Assignment of Numbers to Rank Order Categories. *American Sociological Review*, *35*(3), 515–524. https://doi.org/10.2307/2092993

Learner, S., Thornhill, J., Joiner, S., & de la Torre Arenas, I. (2023). *Quantum computing could break the internet. This is how*. Financial Times. https://ig.ft.com/quantum-computing/

Levinthal, D. A. (1991). Organizational Adaptation and Environmental Selection-Interrelated Processes of Change. *Organization Science*, *2*(1), 140–145. https://doi.org/10.1287/orsc.2.1.140

Lewis, J. A. (2018). *Economic Impact of Cybercrime*. https://www.csis.org/analysis/economic-impact-cybercrime

Lewis, J. A., Smith, Z. L. M., & Lostri, E. (2020). *The Hidden Costs of Cybercrime*. https://www.csis.org/analysis/hidden-costs-cybercrime

Lewis, J. A., & Wood, G. (2023). *Quantum Technology: Applications and Implications*. https://www.csis.org/analysis/quantum-technology-applications-and-implications

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Likert, R. (1932). *A technique for measurement of attitudes*. Archives of Psychology.

Magaldi, D., & Berler, M. (2020). Semi-structured Interviews. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 4825–4830). Springer International Publishing. https://doi.org/10.1007/978-3-319-24612-3_857

Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things (Netherlands)*, *27*. Scopus. https://doi.org/10.1016/j.iot.2024.101228

Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *1*(2), Article 2. https://doi.org/10.17169/fqs-1.2.1089

McCormick, M., & Brower, D. (2021, May 12). *Colonial pipeline resumes operations following ransomware attack*. https://www.ft.com/content/b6ac99ea-d7c6-49dd-b7d7-1284ce2e85c0

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. *1980 IEEE Symposium on Security and Privacy*, 122–122. https://doi.org/10.1109/SP.1980.10006

Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of CyberSecurity*, *2023*, 57–63. https://doi.org/10.58496/MJCS/2023/010

Mind Commerce. (2020). Quantum Computing Market. *Quantum Computing*.

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). *Transition to Post-Quantum Cryptography Standards* (NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547.ipd

Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?* (2015/1075). Cryptology ePrint Archive. https://eprint.iacr.org/2015/1075

Munich Re. (2024). *Cyber Insurance: Risks and Trends 2024 | Munich Re*. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* (SSRN Scholarly Paper 3440802). https://doi.org/10.2139/ssrn.3440802

NIST. (2016). NIST Asks Public to Help Future-Proof Electronic Information. *NIST*. https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information

NIST. (2023). *Digital Signature Standard (DSS)* (Federal Information Processing Standard (FIPS) 186-5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-5

NIST. (2024a). *Module-Lattice-Based Digital Signature Standard* (Federal Information Processing Standard (FIPS) 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

NIST. (2024b). *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (Federal Information Processing Standard (FIPS) 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

NIST. (2024c). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. *NIST*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST. (2024d). *Stateless Hash-Based Digital Signature Standard* (Federal Information Processing Standard (FIPS) 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

OECD. (2019, March 11). *Measuring the Digital Transformation*. OECD. https://www.oecd.org/en/publications/measuring-the-digital-transformation_9789264311992-en.html

O'Reilly, C. A., & Tushman, M. L. (2008). Ambidexterity as a dynamic capability: Resolving the innovator's dilemma. *Research in Organizational Behavior*, *28*, 185–206. https://doi.org/10.1016/j.riob.2008.06.002

Ott, D., Peikert, C., & participants, other workshop. (2019). *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility* (arXiv:1909.07353). arXiv. https://doi.org/10.48550/arXiv.1909.07353

Parenty, T., & Domet, J. (2019). Sizing Up Your Cyberrisks. *Harvard Business Review*, *R1906F-PDF-ENG*, 9.

Peikert, C. (2009). Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, 333–342. https://doi.org/10.1145/1536414.1536461

Pellegrini, A., Bertacco, V., & Austin, T. (2010). *Fault-based attack of RSA authentication*. 855–860. https://doi.org/10.1109/DATE.2010.5456933

Pescaroli, G., Nones, M., Galbusera, L., & Alexander, D. (2018). Understanding and mitigating cascading crises in the global interconnected system. *International Journal of Disaster Risk Reduction*, *30*, 159–163. https://doi.org/10.1016/j.ijdrr.2018.07.004

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012–1236. https://doi.org/10.1364/AOP.361502

Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 208–223. https://doi.org/10.1057/s41288-017-0077-9

Preneel, B. (2005). Hash functions. In H. C. A. van Tilborg (Ed.), *Encyclopedia of Cryptography and Security* (pp. 256–256). Springer US. https://doi.org/10.1007/0-387-23483-7_186

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*, *20*(4), 353–363. Scopus. https://doi.org/10.1108/FS-02-2018-0020

Rajan, D., & Visser, M. (2019). Quantum Blockchain Using Entanglement in Time. *Quantum Reports*, *1*(1), Article 1. https://doi.org/10.3390/quantum1010002

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). *Quantum resource estimates for computing elliptic curve discrete logarithms* (arXiv:1706.06752). arXiv. https://doi.org/10.48550/arXiv.1706.06752

Rogers, E. M. (1971). *Diffusion of Innovations*. The Free Press. https://ocw.metu.edu.tr/file.php/118/Week9/rogers-doi-ch5.pdf

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, *35*(3/4), 260–271. https://doi.org/10.1108/01409171211210154

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students*. https://elibrary.pearson.de/book/99.150005/9781292208794

Sekaran, U., & Bougie, R. (2009). Research Methods for Business: A Skill Building Approach (5th Edition). *International Journal of Information Technology and Management - IJITM*.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Statista. (2024). *IoT connections worldwide 2022-2033*. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Stine, K., Quinn, S., Witte, G., & Gardner, R. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (NIST Internal or Interagency Report (NISTIR) 8286). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286

Swayne, M. (2024, June 18). *IBM Reportedly Partnering With Japan's AIST to Develop 10,000-Qubit Quantum Computer*. The Quantum Insider. https://thequantuminsider.com/2024/06/18/ibm-reportedly-partnering-with-japans-aist-to-develop-10000-qubit-quantum-computer/

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic Capabilities and Strategic Management. *Strategic Management Journal*, *18*(7), 509–533.

Traylor, M. (1983). Ordinal and interval scaling. *Journal of the Market Research Society*, *25*(4), 297–303.

Wang, Y. (2012). Quantum Computation and Quantum Information. *Statistical Science*, *27*(3), 373–394. https://doi.org/10.1214/11-STS378

Weintraub, R., & Borenstein, J. (2017, June 1). 11 Things the Health Care Sector Must Do to Improve Cybersecurity. *Harvard Business Review*. https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity

White, D., & Caralli, R. (n.d.). *100 Days to Build a Strong Cyber Security Foundation*. Axio.

Witte, J. H. (2016). *The Blockchain: A Gentle Four Page Introduction* (arXiv:1612.06244). arXiv. https://doi.org/10.48550/arXiv.1612.06244

World Economic Forum. (2022). *Transitioning to a Quantum-Secure Economy*.

Zängerle, D., & Schiereck, D. (2023). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *48*(2), 434–462. https://doi.org/10.1057/s41288-022-00282-6

Zeller, G., & Scherer, M. (2022). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*, *12*(1), 33–85. https://doi.org/10.1007/s13385-021-00290-1

Zheng, X. (2024). Research on blockchain smart contract technology based on resistance to quantum computing attacks. *PLoS ONE*, *19*(5 May). Scopus. https://doi.org/10.1371/journal.pone.0302325

Appendices

Appendix A: Expert Interviews

Interview Script

The questions below outline the structure that guided the expert interviews. Depending on the depth of knowledge and specialization, the script was adapted to focus on the relevant questions that would maximize quality of insights. Notably, a digression on quantum random generation and quantum key distribution was included thanks to the domain expertise of S5.

1. What is your current knowledge on the development of quantum computers?

2. What are the main applications where quantum computers will be disruptive?

3. How is cyber risk managed, particularly regarding emerging threats?

4. How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

5. What challenges do organizations face in implementing post-quantum cryptography?

6. What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

Summary of Interview: G1

What is your current knowledge on the development of quantum computers?

Nothing is coming to market anytime soon and nobody should be worried. None of the technologies in development today have any reasonable path to building a CRQC. What is important in qubit development is coherence times for gates involving multiple qubits interacting with one another. Even at 1000 qubits, they need to communicate and work together to be useful. You could theoretically make a billion qubits, but they're useless unless they can meaningfully interact with one another. Another issue is error rates. When too high, an arbitrary amount will be bundled together, and the average of their behavior will be called one logical qubit. Now you need to multiply the number of physical qubits by that amount to be useful.

The Google Quantum Supremacy claim was based on a random sampling experiment. For a supercomputer it is very computationally expensive to simulate a large sample of random

numbers, which is essentially the nature of a qubit. All that is needed is to read out from a qubit to extract a distribution, which is not really computing. The claim is that it is faster to sample a physical system instead of simulating the system, which is not relevant to quantum algorithms and exponential speed ups. Rather, it is the sampling of random numbers from a quantum E-Physics experiment.

For the past 20 years, we have been more than 20 years away from achieving a CRQC. We might get there eventually, but the economic incentives are misdirected. The problem lies within the practice of academia in chasing grants and avoiding errors, narrowing conditions to always just maybe be right while demanding more funding and time to run experiments and cover the very high salaries. There is a linear grant model of continuously raising money for experiments, expecting the same timeline of useful results year after year. Microsoft has been investing in QC since 2000 and has the same budget every year. Failing often to get it right quicker, as well as a focus on customer funding instead of grant funding might be more fruitful. However, there is hardly any market incentive since most research funds are coming from governments to break cryptography. There is a niche market on optimization problems, but the technology cannot deliver the necessary capability yet.

What are the main applications where quantum computers will be disruptive?

All the money in quantum is about cybersecurity, more specifically the US and Chinese governments attempting to break each other's secrets with Shor's algorithm – the single algorithm with exponential speed up allowing for the factoring of prime numbers to break RSA encryption. AI for quantum and applications in drug discovery and finance are just smoke screens and most revenue is coming from government or its proxies.

How is cyber risk managed, particularly regarding emerging threats?

Hypotheticals that could happen one day are generally not a high priority. If a company had a data breach due to some attack and the impact becomes easily quantifiable, then it becomes an immediate fix and budget becomes irrelevant. In the example of the Solar Winds attack, a very hard task was done within weeks.

What challenges do organizations face in implementing post-quantum cryptography?

Upgrading cryptography standards of data moving live today could happen very quickly. Meta changing HTTPS encryption from RSA to elliptic curve takes no time at all, and consulting companies like Accenture will gladly handle this. Most software deployed today gets continuously updated and can receive air updates into cars or devices for example. The

problem lies mainly in older devices that are more than 10-15 years old, made in the pre-2008-2010 era. Consulting projects will be necessary to go over the entire software inventory and discover necessary changes, which is very time consuming. However, once all is discovered, it is very much plug and play.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

The rate of adoption is likely low and not even driven by fear of quantum computing, but rather by the need of updating defaults and tools in use – cybersecurity is generally very reactionary. To accelerate the adoption of PQC, someone would need to get hacked by a quantum computer. The SNDL threat matters more to state secrets and personal communication, and less for banking transactions or IP Protection. Most IP has likely already been stolen at state levels.

There isn't a lot of encryption that can't already be broken today. Quantum computing will make it easier, but if the intelligence community wants to break some secret, they will put a lot of resources into eventually achieving it. For example, Snowden has leaked the NSA having purchased a backdoor into RSA encryption, potentially having been a part of their business model.

The first movers to upgrade cryptography are financial institutions or instances storing personal information linked to assets like social security numbers. Companies involved in cryptography and providing certificates like Verisign (a spin off from RSA) are already integrating quantum safety and there is big business in helping organizations switch their encryption, considering the slight chance that a CRQC could be just few years away.

Summary of Interview: G2

What is your current knowledge on the development of quantum computers?

Current data is not reliable enough to make accurate predictions about the future. It could be 10-15 years to achieve a CRQC, but with a large error margin. However, as has been observed with the development of Artificial Intelligence, things always move slower in the beginning as expected, and faster towards the end.

How is cyber risk managed, particularly regarding emerging threats?

The equation for risk is likelihood times impact. The risk of quantum computing is difficult to quantify because the impact is enormous and timing unknown. We are generally not good in dealing with high impact, low likelihood events, as observed during nuclear or natural disasters.

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

It is generally accepted that the government and financial sectors are most aware and affected. Government for obvious state secret reasons, and financial institutions due to anticipation of coming regulations on this topic. Telecommunications would be next in line.

What challenges do organizations face in implementing post-quantum cryptography?

Action will vary depending on the organization. If everything is stored on the cloud or third-party software products are in use, the vendor will need to be relied on for updating the cryptography. Others like Meta have a crypto stack built from scratch or using existing libraries, which would require changes on internal systems. However, complex infrastructures can take (even ten) years to migrate.

Most of cryptography is anything but plug and play. A lot is hard coded for example in legacy systems that are no longer maintained. Cryptography is at the very bottom of the stack and downstream impacts need to be tested for. Another big problem in cybersecurity legacy in general are supply chains and dependencies on other organizations to migrate an interoperating system, often causing inertia or inaction. The new PQC algorithms also have downsides which need to be considered.

Generally, the entire infrastructure needs to be upgraded since cryptography is embedded in the bedrock of every communication between two machines. There are limited workarounds only applicable to some use cases.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

Risk and compliance are the main drivers for adoption. Industry is not regulated yet, though financial institutions work on awareness to allocate budgets and create momentum to address the risk. Federal agencies on the other hand are mandated by the US Government to take action (Quantum Computing Cyber Security preparedness Act).

Compliance has an important role to get things going. Regulated industries will move faster on this topic but not necessarily do the right thing. Their learnings will allow other industries to eventually pick up and shift action from compliance to actual risk mitigation.

Summary of Interview: G3

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Big tech corporations and banks are very aware, whilst companies in other industries like automotive are less concerned.

What challenges do organizations face in implementing post-quantum cryptography?

Companies like Google which own the entire technical stack can switch in a matter of a year or so, but that doesn't apply to everyone else with external dependencies. While application clients like VPNs can be updated on the laptop for example, the laptop itself might need to be replaced as well, as many computing platforms use RSA or ECC hardware accelerators.

The entire infrastructure needs to be replaced, as expired certificates won't be accepted anymore. Software patch can function as a temporary solution, but hardware needs to be replaced in long run.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

The federal government mandates PQC, hence the entire government market is required to comply and upgrade its cryptography. Most internet communications like internet protocols already include PQC.

Cost is a big factor, since there is no tangible ROI. Wouldn't be surprised if after 15 years some people didn't switch yet.

Most companies that intended to implement the NIST standards already have a version of implementation, as a draft was released one year before the final publication. Now they can be officially integrated into their systems. However, it is not an immediate action, but rather a continuous effort.

Summary of Interview: G4

What is your current knowledge on the development of quantum computers?

We have historically repeatedly underestimated the evolution timeline of technology, thinking of progress as linear. While most are focusing on superconducting qubits, there are many different technologies that are being betted on, including photonics-based or spin qubits. Advancements in research might occur faster in some than others, but for predictions, most people consider the superconducting qubit timeline and observe the two biggest companies – IBM and Google. In general, the biggest challenges in quantum computing development are scalability and error correction.

Most funding comes from governments, considering the dual-purpose of this technology with applications in defense and other state interests. An initial boost is needed as this technology falls under deep tech long term investments using patient capital, although a significant amount of funding does come from corporations in the USA and Japan.

All the focus is on a quantum Computer breaking RSA in seconds. However, other methods could arise, like the combination of high performance and quantum computing that could break RSA in minutes or hours perhaps, potentially reducing the relevance of a fully scalable CRQC.

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Awareness depends on geography, as developing and emerging nations have not been considering quantum computing at all. Nations that have started the journey on quantum have raised awareness especially with defense and related sectors. Next up would be banking and financial services, including insurance, followed by energy, transportation and infrastructure, as well as health care and pharmaceutics. Finally, the rest of the consumer sectors will be laggards with much later deployment.

The banking industry will be most significantly affected, as financial transactions lie at the root of every industry. The SNDL threat is more related to data relevant for national security, potentially touching corporate IP and trade secrets as well. Cyber-attacks are very coordinated nowadays, with international and even state sponsored operators. It can become increasingly complex to assess which kind of data will be relevant and targeted.

What challenges do organizations face in implementing post-quantum cryptography?

The implementation needs to be tackled holistically, in all infrastructure and applications. The first step is discovery in understanding what needs to be updated. Organizations like banks have numerous legacy applications, mainframes with different versions, and purchased applications from vendors, posing a massive discovery exercise. There are intermediate solutions including function wrappers for the interim period, which many third-party solutions providers are working on. Organizations should also analyze where they can make their systems more modular for the next time a change of algorithms is required. The NIST PQC algorithms might change moving forward and none of them have actually been tested against a quantum computer. Security is always a moving target.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

Transition to PQC will be complex and expensive. Most of startups in India working in security are already using PQC standards, which are typically always followed by the cybersecurity community.

Summary of Interview: G5

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Post-quantum is not as big a topic within Risk Management. However, when assessing compliance, cryptography is usually a topic, particularly regarding key management or the lack thereof. The Automotive industry is concerned due to the future data integrity of autonomous driving and the interest in protecting its products from potential attacks.

What challenges do organizations face in implementing post-quantum cryptography?

It is important to distinguish between a cryptographic primitive and the method. For example, AES is a method while the mathematical problem is factorization. A method could become insecure without the mathematical problem being the root, but rather poor implementation on certain parameters like key lengths for example. Also, the constant increase in key sizes could lead to a dead end and has never been tested against a quantum computer running Grover's algorithm, remaining a speculative solution.

Exchanging algorithms from Libraries is not as simple in practice, demanding a huge bureaucratic effort to assess where cryptography is implemented. For example, the hash

function SHA1 has been classified as unsafe since 2015, yet it is still in use and supported by TLS, with a planned phase out in 2030. There are initial tools for cryptographic inventory assessment in communications applications to scan for the usage of keys and certificates. However, there are many instances that can't be scanned as with hard drive encryptions like BitLocker for example. Companies need to assess and prioritize applications and critical information by security risk.

Migration happens on 3 levels:
- Owned applications need to be internally reworked, which can become complicated if dependencies between applications are involved
- Standards like TLSS need to be centrally adapted by working groups and can't be migrated by oneself
- Finally, everything needs to be orchestrated to function harmoniously. The key management system needs to be able to change keys and provide the appropriate method to ensure agility.

It is possible to floodgate certain legacy systems and disconnect them from communicating over the internet.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

There is no big wave of adoption yet, but rather just explorative actions for now. With the release of the new standards, momentum has slowly been ramping up, and post quantum and crypto agility are becoming more frequently requested topics for consulting services. For the financial industry, regulation is a big driver for adoption. The automotive industry is regulated as well, although the focus is more directed towards safety and reputation of product integrity.

The PQC algorithms are not definitely quantum-safe, since they have not been tested against a CRQC yet and there are potentially new algorithms yet to be discovered. The chase between encryption and decryption algorithms is gaining pace, and while cryptography used to remain safe for hundreds of years, recently the cycles have decreased to decades and will likely accelerate even more. While testing the NIST algorithms for time (10 years of testing passed since the call for proposals), crypto agility and hybrid solutions will be the way forward.

Irrespective of the opinions on the development timeline of QC, it doesn't hurt to invest into cryptography and discover security gaps now. Thinking beyond QC, progress in Artificial Intelligence may also create new threats. Of the 4 NIST algorithms originally proposed, one was broken by a classical computer and had to be removed.

Summary of Interview: G6

What is your current knowledge on the development of quantum computers?

Quantum computing will not be able to replace classical computing. A lot of money has been injected into this technology; however, qubits are still very erroneous and difficult to scale functionally. On the flipside, real progress in quantum computing development is difficult to assess due to geopolitical obscurity.

How is cyber risk managed, particularly regarding emerging threats?

Security is never a priority for companies until they are under attack.

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Many organizations neglect the QC threat. However, governments, the financial domain, and all entities relying on identity management are concerned and working on implementing the NIST standards. Since the US government mandate on quantum safety, more companies have been starting to act.

Hardware that remains in the field for 10 or 20 years, like cars and passports for example, could be at risk considering the CRQC date projected around 2030 or 2035. Taking the example of the car, potential exploits could be a connected mobile phone which is linked to a payment service, hijacked during a financial transaction. A compromised firmware update on the car could be signed by a broken key, or a Denial of Services could be performed on all cars of a manufacturer. Authentication is critical in terms of quantum security.

What challenges do organizations face in implementing post-quantum cryptography?

Governments in some European countries propose creating cryptographic inventories. Once all the assets using cryptography have been identified, a risk analysis is performed, linked to the timeline of data confidentiality. Finally, a migration plan is defined considering flexibility or crypto agility, which is challenging to implement and can take years.

As the NIST algorithms have only been recently released and not tested for time, it is recommended to use hybrid cryptography composed of 2 layers of security. This requires the handling of both algorithms as well as the mechanisms guaranteeing safety when replacing and algorithm. Hence, even with air updates, IoT devices require preparation for quantum-

safe hybrid cryptography to handle the added complexity and compute. The larger key sizes of lattice-based algorithms increase memory requirements and the communication payload (bandwidth) by 5-10x.

Legacy devices can be revoked based on their unique identifiers, or basically killed, if not updateable.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

Adoption will depend on the country and its regulations, applying pressure by prohibiting sales if not compliant. For US Government products and services, quantum resistance is already integrated into the design. There has been an increasing demand of customers asking for quantum resistance within the past half year.

The main obstacles are large expenses in labor and a lack of competencies or talent. Amplified with the fact that security is never the priority for an enterprise.

Summary of Interview: G7

What challenges do organizations face in implementing post-quantum cryptography?

Some industries can deploy PQC very easily and quickly.

The compute time for PQC and classic factorization algorithms is similar. However, the size of keys and ciphertext is significantly larger, in some cases by a factor of 10, which can be limiting for some applications.

The implementation of PQC is harder to randomize than classic factorization algorithms as more elements are involved. A complete implementation that protects against side-channel attacks (requires physical access to device) can be 5-6x slower.

If an IoT device can’t be updated over the air, it needs to be replaced. Generally, devices used for authentication are not as critical. Those that are used for encryption on the other hand need to be upgraded as soon as possible.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

When reviewing banking applications, cryptography from before the 1990s was still being used (by MasterCard and Visa) due to reasons of legacy compatibility. Since the old standard

is still regarded as secure, nobody can mandate the banks to update. On symmetric crypto, some are still using 3DES instead of AES. Hence, adoption will depend on the industry and level of regulation.

Summary of Interview: G8

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Within cryptographic circles, awareness is very high. There is a lot of buzz and awareness is starting to spread, amplified by the NIST mandating changes in government systems. However, while most people have an idea, awareness is generally still low.

NIST has set deadlines for the US government to deprecate old algorithms (RSA & Elliptic curve). Hence, to deliver products to the US government, one's products need to be migrated to PQC. Australia has set the same deadlines for their government.

What challenges do organizations face in implementing post-quantum cryptography?

For large organizations, migrating to PQC is a lot of work, considering the thousands of applications and legacy systems involved which need to be classified and updated. Complete migration can take 20-30 years. Either all the applications are internally developed and need to be internally updated, or external vendors are involved, in which case some older applications might not even be supported anymore.

As seen historically with SHA1 (deprecated over a decade ago) and DS (classified unsafe 30 years ago), which are still used by some legacy applications, the full adoption of new standards can take a very long time.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

First movers in adoption are government, the financial industry and telecommunications (6G will only use PQC). While there are no regulations of PQC yet, many regulations mandating cyber hygiene imply the upgrade of cryptography. Furthermore, larger institutions like Santander Bank are taking the lead and supporting smaller ones with lesser resources.

A barrier to adoption is standardization. While the NIST algorithms have been released since August 2024, the implementation is not yet fully standardized, for example in the use of TLS

connections. As the drafts won't be final until late 2025, real migrations for real use cases will begin picking up from 2026.

Furthermore, there is a huge talent shortage, resulting in scarce cybersecurity resources which need to be carefully prioritized.

Summary of Interview: G9

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Quantum is one of those risks that we know about and that could have a really big impact. On the other hand, experts clearly disagree on the timeline of when this technology matures, whether in 5, 10, 15, 20 years or never. The focus should be less directed towards the quantum threat but rather getting the foundations right. Improving the maturity level of managing and implementing cryptography will alleviate migration to post-quantum down the road.

Generally, while some organizations have been proactive in starting quantum migration initiatives, the general sentiment is that this kind of risk is significant, but not urgent. Some resources will need to be allocated to start planning for it, but there are many more immediate threats that may get one's business compromised within a shorter timeframe.

It is unlikely that a quantum attack would be available to an opportunistic criminal threat actor to attack a business anytime soon, considering the current state of public research. If a quantum breakthrough were to happen within the scope of a major government, it would certainly be classified and used very selectively to obscure the capability. For operating a normal business, the threat is not as immediate.

What challenges do organizations face in implementing post-quantum cryptography?

The biggest task is the cryptographic inventory assessment and definition of right processes, whilst ensuring everything functions harmoniously.

A lot of the new algorithms are not drop-in replacements for the old ones, as performance considerations need to be taken into account. In a more constrained environment, larger key sizes and bandwidth requirements could lead to operational impacts.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

While there is no PQC mandate on a European level, there are directives that set minimum requirements for cybersecurity across critical sectors. For example, in the financial sector, the DORA regulation sets functional requirements such as a management system for cybersecurity, risk management and operation within an acceptable risk level for critical digital services. What is currently on the table is the preparation for post-quantum migration and readiness within a 10-15 year time frame.

Adoption is currently growing organically, with momentum added by the release of NIST standards. post-quantum support is being increasingly built into software libraries and products and an option. However, backend and legacy systems will likely require a longer time to fully migrate.

Summary of Interview: S1

What is your current knowledge on the development of quantum computers?

It is hard to predict the future, but people are saying that a useful QC could be achieved between 2027 and 2035. One should closely monitor the progress of leading companies in delivering on their roadmap.

There are several layers to the development maturity of quantum computers:
- Quantum Supremacy: A quantum computer outperforming a classical computer. Most agree that this has already been achieved by Google in 2019. However, it was misleading since the calculation was completely useless.
- Quantum Utility: A quantum computer solving a useful problem that is not commercially viable, for example for research and discovery.
- Quantum Advantage: A quantum computer solving problems with real world applications, for example in simulating molecules for chemistry, optimization problems in finance and energy distribution, or cryptography.

Quantum advantage is still a few years away. Currently, the industry is still in its research phase and has not reached maturity yet, necessitating public funds to drive development. There is not much private investment as it is a long shot technology.

There are several other platforms to superconducting qubits like trapped ions, photonics, or neutral atoms, which might become dominant with some breakthrough. Besides the number of qubits, an important quantum benchmark is fidelity, which describes the resistance to errors. Trapped ions have a very good fidelity, but it is difficult to combine more than 30 qubits. Hence, there is a trade-off between fault tolerance and scalability. Cost is also a big factor to take into account. Superconducting qubits are relatively easy to manufacture, require merely the printing of a quantum chip using existing semiconductor capabilities. Trapped ions on the other hand, require a special magnetic construction which requires R&D from scratch.

What are the main applications where quantum computers will be disruptive?

A big use case will be in finance optimization problems, for example within portfolio management. Small improvements in network related mathematical problems, as applied to large scale industries like logistics will also have big impact. For example, airlines calculating optimal flight routes to save fuel, or maximizing efficiency of public transport in cities. Another application would be the simulation of molecules, with use cases in pharmacology for the development of new drugs, or in chemistry for battery development for example.

However, as the technology hasn't reached the level of computation necessary to provide tangible competitive advantages in real-world applications yet, clients are mainly using the current state of the art for training purposes. Some will purchase quantum computers, but most just hire cloud computing time to become familiar with the technology and be prepared for the day that it eventually matures.

Summary of Interview: S2

What is your current knowledge on the development of quantum computers?

Quantum computers today are nowhere near close to breaking encryption. NVIDIA's CEO having claimed QC to be 15 or 30 years away could very much be true. A lot of hype is being generated by vendors who are financially incentivized to, as Google's did with their Willow announcement in late 2024. Quantum startups will exaggerate progress to secure funds, and security companies will scare you to get your business.

In terms of investment into the technology, it will be around 10% of generative AI. However, there are still significant challenges to be overcome until vendors are anywhere close to achieving useful quantum computers. The more qubits are added, the harder it becomes since

they need to network together. IBM achieved 1000 qubits, but it is still a very long way to 100.000 qubits, which is the scale at which it becomes useful.

Another problem is the number of computations a qubit can perform, described by coherence times. As quantum states are inherently unstable and interact with the environment, the integrity of information held in a qubit degrades over time. Superconducting qubits are very fast but very limited in number of operations. On the other hand, trapped ions and neutral atoms are much slower but have much lower error rates and longer coherence times. Hence, there is a trade-off between coherence time and computation speed. There won't be just one platform for quantum computing. Instead, there will be many different configurations depending on the use case and budget, energy and time available to perform the calculations.

What are the main applications where quantum computers will be disruptive?

Many companies lie and claim use cases for 2-digit numbers of qubits, but there are none. One of the earliest applications will be in chemistry, for example the simulation of physical processes or a molecular reaction. To illustrate, simulating one caffeine molecule with the electronic structure of hydrogens, carbons and oxygens, would require160 perfect logical qubits. However, logical qubits can be loosely defined and range from 2 to thousands of physical qubits. Let's say that one logical qubit is composed of 1000 physical qubits. It would hence require 160.000 physical qubits to just represent one molecule. A good use case could eventually be the improvement in efficiency of lithium batteries. However, the required number of qubits will be at a similar order of magnitude as necessary for breaking encryption. The current use cases of quantum computers are experimentations to learn how to use them.

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

For the past 8.5 years, people have been working on post quantum. It is possible that somebody could find a new attack using QC or classical computing even on the new NIST standards, which is why they continue the process of getting new candidates. All of the focus is on factorization performed by a QC, but there is no proof that this might also be done more efficiently using a classical computing method. There are no guarantees, which is why cryptographic agility is such a critical part of the process. One should not just simply switch the encryption schemes, but rather transition to a cryptographically agile environment, as in five years, the current NIST algorithms could become obsolete.

Summary of Interview: S3

What is your current knowledge on the development of quantum computers?

Quantum computers still lack the capabilities for significant ROI on this technology. Many different platforms are being explored, but it is uncertain which will win. There are also diverging approaches, either specialized on certain use cases, or more generalized for larger applications like IBM is aiming for.

While China might be a lot more advanced than they are communicating, generally, progress in this technology can be publicly followed by observing the leading companies IBM and Google, with Microsoft following suit. IBM has strong transparency on the advancement of their research, and they open sourced their software technology with the benefit of accelerating progress. Google did achieve a real hardware advancement in error correction with their recent announcement end of 2024. However, the quantum supremacy claim was misleading as the underlying calculation was completely useless. Generally, the term quantum supremacy doesn't make sense, since quantum computers will never replace classical computers, both serving different use cases. While quantum utility has been demonstrated by IBM in 2022, quantum advantage is the next milestone.

What are the main applications where quantum computers will be disruptive?

Within IBM, the quantum business applications are Quantum AI, Optimization and Simulation. Quantum AI is already tackling business problems at scale, enhancing AI algorithms with real world pilots for banking applications since 2023. However, the expected value is still small compared to the potential in other domains, leaving most clients to question the ROI of quantum hardware investments at the current stage. Quantum simulation allows for the simulation of a quantum computer on a classical computer, which many companies today use for exploration and specific cases. Few early adopters who believe in the technology and are interested in the early path to industrialization and maturity do deploy quantum hardware within their enterprise. However, sovereignty topics around this technology limit hardware contracts mainly to public institutions in few countries besides the US, including Japan, Germany and Spain.

Most clients today contract a cloud offering, granting access to real hardware without the need to invest in a quantum data center and the customized infrastructure around it. As the technology matures, becomes backwards compatible and price decreases, hardware investments will become more interesting.

The first use cases will be in financial services, pharmaceuticals, and chemistry, followed by the aeronautical, big logistics and energy & utilities industries, solving problems of design, optimization and simulation. Taking the example of the traveling salesman problem, in which the smallest travel distance with the highest value is to be optimized for based on many parameters, for a major logistics company, just a 1% efficiency gain could lead to a value increase by a factor of 2. Hence, a 10-20% efficiency increase can become very disruptive in terms of significantly outperforming competitors. IBM aims to achieve this by 2030.

Summary of Interview: S4

What is your current knowledge on the development of quantum computers?

If a state actor had the capability to break encryption, it wouldn't necessarily become public knowledge immediately. Where budgets are unlimited and state secrets are involved, facts will be obscured for a while, as has been the case with Enigma.

How is cyber risk managed, particularly regarding emerging threats?

When running a CISO organization, based on the headcount and technologies to be refreshed, a budget will be proposed on a yearly basis. A live document called a risk register will be adapted to the ever-changing risk landscape and inform decisions, though budget will not be adjusted on a monthly or quarterly basis. Frameworks like SAFe will approach risks from a quantitative perspective. With qualitative approaches risks will be assessed and prioritized by likelihood and impact, while allocating funding and defining owners for mitigative actions.

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Some organizations are starting to allocate some funds for initial exposure assessments or studies on implications on the enterprise or architecture. However, big companies are usually driven by emergencies and wait until the last minute, whilst struggling with understanding the severity of risks like SNDL. The shelf life of data and the level of impact can vary greatly depending on the use case. However, when data protection lifetimes are mandated by global regulators, things can become tricky.

What drivers and obstacles affect the adoption of post-quantum cryptography and what is your projection?

Not every industry is regulated globally like financial services and insurance. Hence, it won't be a universal driver for most industries. While regulation drives expenditures and actions, other risks should not be overlooked by practicing security by compliance.

Since the release of the NIST standards in August 2024 interest for preliminary assessment has increased, amplified by Chinese real or misinformation claim of having achieved a CRQC proof of concept. The groundwork for road maps and changes across enterprises is being rolled up into CISO strategies and budgets over the coming years.

Summary of Interview: S5

How would you assess the level of awareness and preparedness on quantum computing's encryption threat?

Since the release of the new NIST standards, awareness has been rising in the market. Specifically, within the verticals of government, military, and the financial industry, awareness levels are really high.

What challenges do organizations face in implementing post-quantum cryptography?

Most crypto is embedded into the code of applications, making it very unflexible to migrate. Rewriting code and embedding new algorithms natively into applications can take up to decades. The first step is assessing what crypto is in use. Most organizations just trust the vendor and don't have an overview over their crypto inventory.

The times of using the same crypto for over 30 years is over. In the future, it might need to be changed every second year, requiring flexibility or crypto agility in the system's architecture.

Digression on quantum random generation and quantum key distribution

12 years ago, the only way to address the quantum threat was through QKD, which meant completely getting rid of mathematics.

<u>Quantum Random Generation:</u>

As all cryptography is generated out of randomness, the higher the quality of randomness, the stronger the security. Most companies are not using proper methods to generate crypto objects, resulting in poor entropy. The inherently random nature of quantum mechanics poses a superior alternative to seed the generation of existing or post-quantum crypto and is already widely adopted today.

Quantum Key Distribution:

For some customers, the uncertainty within the security of mathematical encryption methods and regularly required updates is unacceptable. Companies in industries like government, defense and finance, requiring long-term data confidentiality guarantees, want the problem solved indefinitely - which is only possible by removing mathematics.

QKD was invented in 1984 but only found adoption around 10 years ago. It is expensive and complex and has limitations that can't address all use cases. A physically connected quantum channel is required and while distance limitations can be bridged by trusted repeaters, connection between continents becomes more difficult and may need involvement of satellites. Hence, it is generally used to protect the backbone as a secure network, complemented by PQC to protect data within end-to-end devices. However, it provides certainty that data will be protected for many decades, as any interception disrupts the quantum state and leads to immediate detection. The only security risk lies within the vendor, which needs to be trusted not to implement any side channels or backdoors. Standardization bodies are working towards interoperability, but today the technology can only be deployed by a single vendor.

Appendix B: Survey Outline

#	Question	Question Type	Answer Options
	Screening questions		
1	What is your role?	Multiple choice	C-Level; IT Director; IT Generalist; Cybersecurity Specialist; Other
2	What industry do you work in?	Multiple choice	Financial Services; Healthcare; Transport & Logistics; Chemicals & Pharmaceuticals; Industrial Manufacturing; Government & Military; Technology; Energy & Resources; Motor Vehicles; Consumer Goods; Telecommunications; Other
3	What is the size of your organization?	Multiple choice	<1000; 1000-10.000; 10.000-50.000; 50.000+
4	Where is your organization headquartered?	Multiple choice	List of Countries
	Awareness & perception of quantum threats		
5	How familiar are you with the impact of quantum computing on cybersecurity?	5-point Likert scale	Not familiar at all (1) – Expert (5)
6	How familiar are you with the Store Now, Decrypt Later (SNDL) threat?	5-point Likert scale	Not familiar at all (1) – Expert (5)
7	How familiar are you with the concept and practice of crypto agility?	5-point Likert scale	Not familiar at all (1) – Expert (5)
8	How concerned is your organization about security risks posed by quantum computing?	5-point Likert scale	Not concerned at all (1) – Extremely concerned (5)
9	In what timeframe do you expect quantum computers to become capable of breaking widely used encryption methods such as RSA, ECC, and DH?	Multiple choice	<5 years; 5-10 years; 10-15 years; 15+ years; never
	Current encryption practices & quantum readiness		
10	How thoroughly has your organization assessed its use of encryption (cryptographic inventory)?	5-point Likert scale	Not at all (1) – Fully assessed (5)
11	What asymmetric encryption algorithms does your organization use?	Multiple choice (multiple selection possible)	Uncertain; None; RSA; ECC; DH; ML-KEM; Hybrid
12	This question was placed to validate your attentiveness. Please simply answer with "Crypto Agility".	Quality control	Quantum Computing; Quantum Key Distribution; Post Quantum Cryptography; Crypto Agility; Public Key Infrastructure
13	Does your organization rely on third party solutions for cryptography management?	Multiple choice	Uncertain; No; Yes
	Risk exposure and management		
14	How would you assess your organization's exposure to quantum security risks?	5-point Likert scale	No exposure at all (1) – Full exposure (5)

15	How would you assess the potential operational disruption quantum computing could cause to your organization?	5-point Likert scale	No disruption at all (1) – Full disruption (5)
16	To what extent is the quantum threat integrated into your organization's risk management strategy?	Multiple choice	Not addressed at all; Slightly (no actions taken); Moderately (limited planning); Significantly (mitigation strategies in place); Comprehensively (clear action plan); Uncertain
17	How long does your organization's data need to be kept confidential?	Multiple choice	0-5 years; 5-10 years; 10-15 years; 15+ years
18	When does your organization plan to begin transitioning to Post Quantum Cryptography (PQC)?	Multiple choice	Already begun; 0-5 years; 5-10 years; 10-15 years; 15+ years; Never
19	*Dependency: Q18 "Never" not selected:* How long do you estimate your organization's transition period to PQC?	Multiple choice	0-5 years; 5-10 years; 10-15 years; 15+ years
20	How is your organization allocating budget for PQC?	Multiple choice	No budget allocated; Minimal budget (exploratory funding); Moderate budget (research & planning); Significant budget (implementation efforts); Dedicated budget (strategic priority); Uncertain
Adoption factors			
21	Rate the significance of the following factors to your organization's action on adopting PQC: Potential regulation / compliance mandates; Budget constraints; Talent shortage; Process constraints; Availability of standards; Competitor moves; Availability of third-party vendors; Quantum Computing technology leaps; Reputational impact	5-point Likert scale matrix	Insignificant (1) – Extremely significant (5)
22	*Dependency: Q18 "Already begun" not selected:* Does your organization plan to wait for regulatory mandates before transitioning to PQC?	Multiple choice	Uncertain; No; Yes
23	How dependent is your organization on third party suppliers to transition to PQC?	5-point Likert scale	Not dependent at all (1) – Extremely dependent (5)
24	(Optional) What would make the adoption of PQC easier for your organization?	Text input	-

Table 5 Outline of survey questions