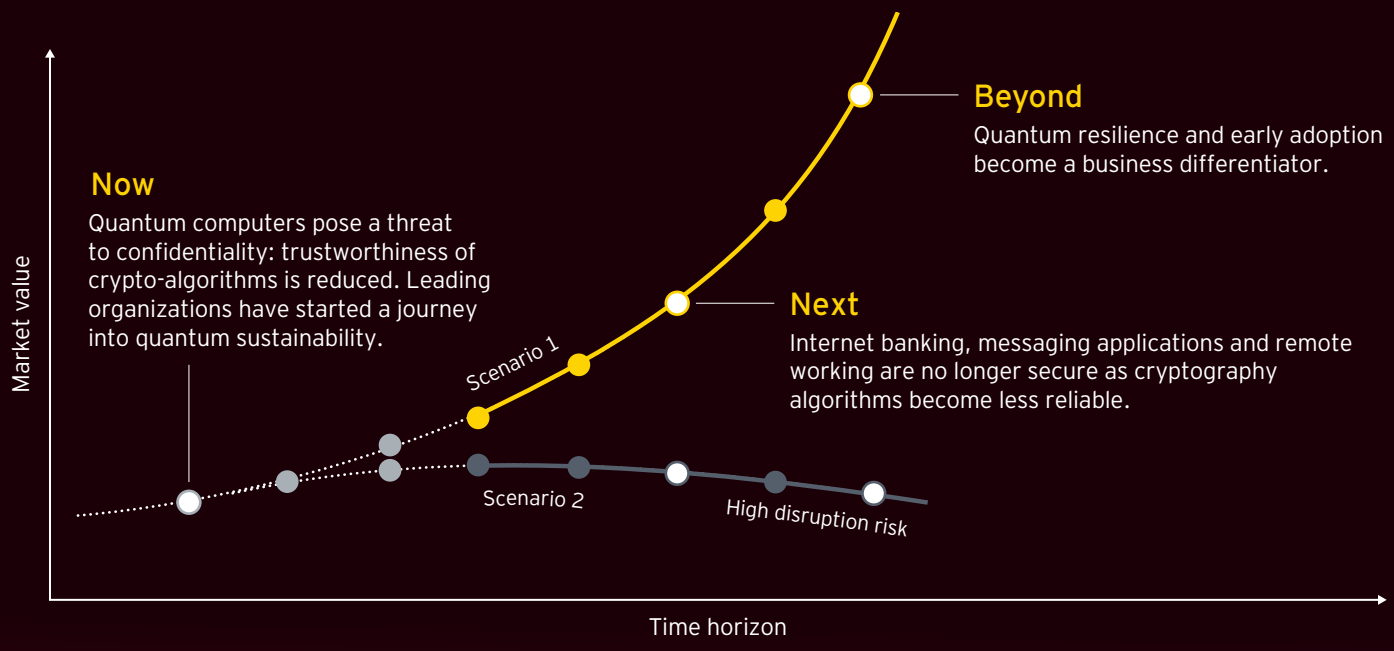

Quantum computers will break the existing confidentiality paradigm. The only question is when?
The better the question. The better the answer.
The better the world works.
EY
Building a better working world

Quantum computers pose an existential threat to cryptography — the foundational control to ensure data confidentiality.



Now

Quantum computers perform certain complex computations much faster than classical computers. Its ability to solve previously unattainable problems brings advantages and risks.

Today's organizations rely on encryption to secure their data. The strength of current cryptography algorithms is based on the computational complexity of specific mathematical problems. Those problems are no longer hard with the presence of a quantum computer. Quantum computers pose a threat to confidentiality, reducing the trustworthiness of crypto-algorithms.

Cryptography is built into every application. The omnipresence of cryptography makes the quantum-in-cyber risk pervasive. A major infrastructure change is required to remediate the quantum threat. These changes cannot be done overnight.

Regulators have already started developing quantum-resistant cryptography algorithms. Organizations where data is a key asset and confidentiality is critical to business success have begun a journey into quantum sustainability.

Next and Beyond

Scenario 1

- Leading companies have become quantum resilient through adoption of technologies that have kept them secure and given them a competitive advantage.
- Changes have been implemented in a rational and stepped way with deep analysis of business needs.
- Confidentiality of data at rest and in transit is accomplished using post-quantum cryptography.
- Budget spending going as planned.

Scenario 2

- Companies that did not take preliminary steps to secure functions such as internet-bank applications, messengers and remote working platforms cannot protect users' data.
- Hasty changes in the infrastructure, and across critical applications and services are disrupting business performance.
- Budgets are not ready to meet changes at pace.
- Business accepts critical risks.

Quantum is not an agenda for tomorrow, but for today.

Regulatory response

The US National Security Agency (NSA) has recognized the existential threat quantum technology poses to encryption. In 2016, the NSA published a memo dictating that the Committee on National Security Systems (CNSS) should no longer use five traditional encryption methods as they are compromised by quantum computing technology.[1]

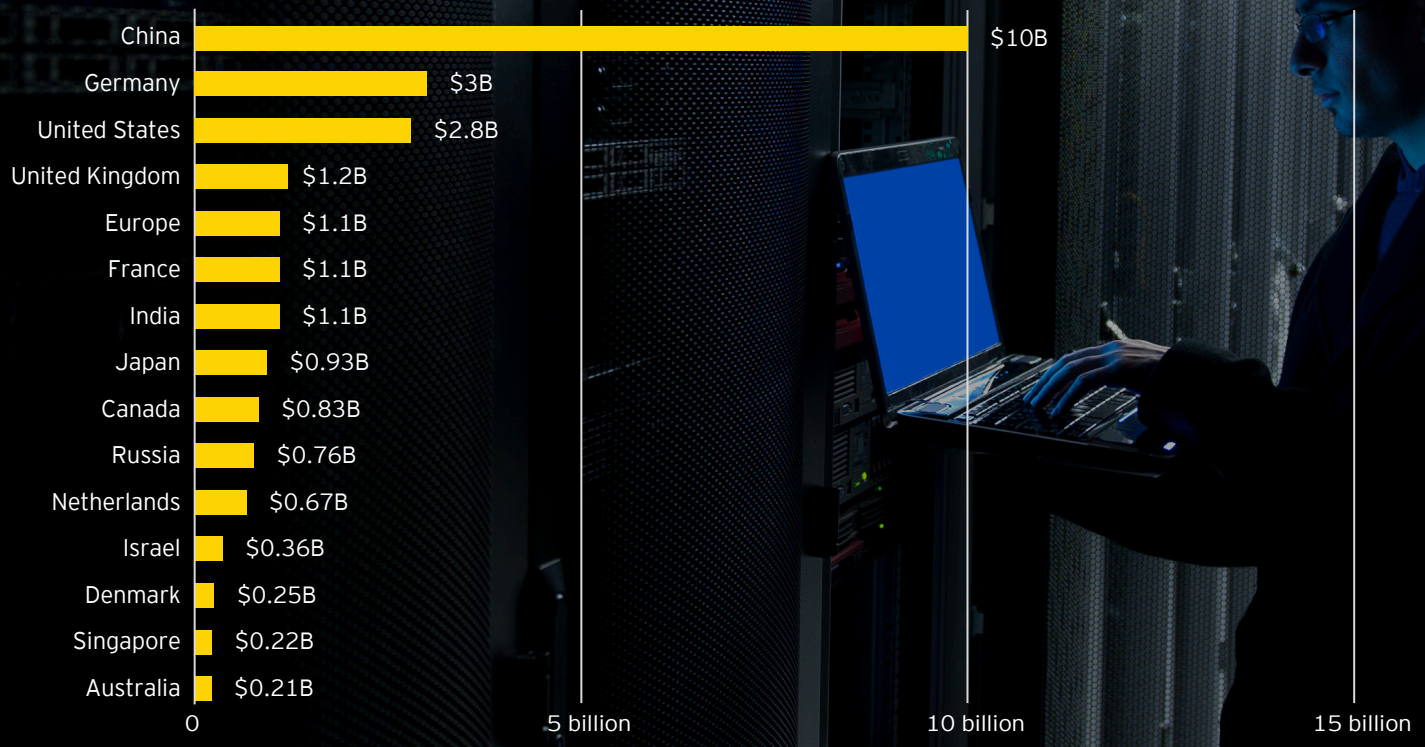
In 2018, the National Institute of Security Technology (NIST) started the development of cryptography algorithms that could withstand an adversary with access to the quantum computer. Multiple review rounds have narrowed the selection to four algorithms as candidates for standardization, with a decision planned for 2023.[2]

Who is investing now?

Investment in quantum computing has increased exponentially. Governments and corporations around the world are investing billions on developing quantum computing – it has been recognized as both a significant security risk and a commercial opportunity.

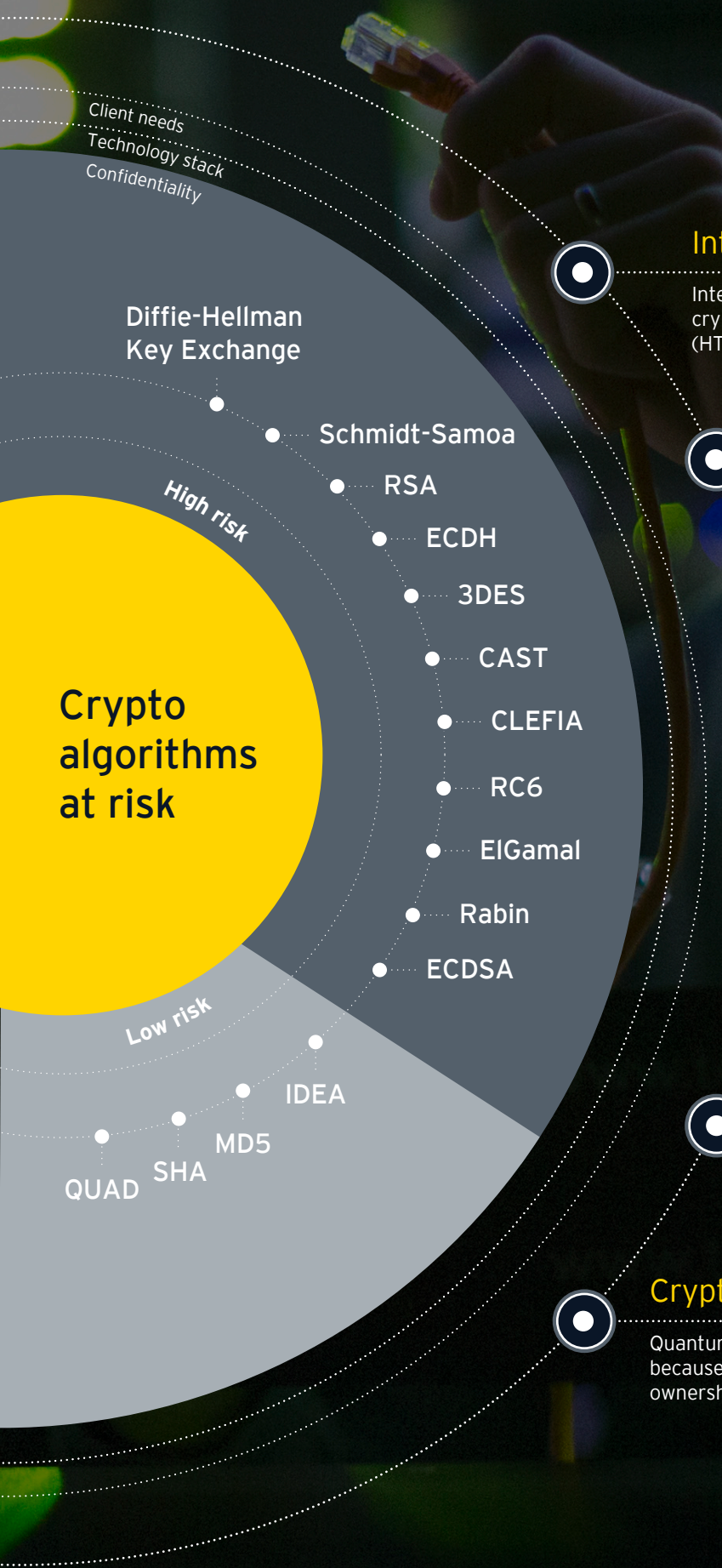
- Governments around the world, such as the USA, Russia, China and Australia, are spending a significant amount to develop quantum computing capabilities.
- Technology companies are also heavily investing in quantum technology. For example, Google and IBM have clear roadmaps on quantum business applications reliant on the number of entangled qubits.

Recent government funding announcements for quantum research & development[3]



[1] https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf
[2] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline
[3] Based on **"The Quantum Insider"** information.

Common business applications and consumer services will be rendered vulnerable.



Internet banking

Internet banking applications heavily use asymmetric cryptography to encrypt connections between client and server (HTTPS) and authenticate transactions (digital signature).

Messaging applications

Data confidentiality in messaging applications is based on cryptography algorithms that are vulnerable in the presence of an adversary with a quantum computer.

Internet of Things

Every IoT device communicates with its parents via HTTPS connection, which involves vulnerable cryptography.

Remote working

Virtual private networks (VPNs), which underpin remote working infrastructure, will be susceptible if not modified.

Commercial in confidence

Information, such as board papers and financial reports, which is usually protected by cryptography protocols, will become insecure.

ATM transactions

ATM transactions are complex, involving interactions between various technologies. Confidentiality and integrity of those transactions is based on asymmetric encryption protocols and thus vulnerable.

Crypto currencies

Quantum computers pose a risk to blockchain-based solutions because they can recover a private key, which is used to prove ownership, from publicly available information in the chain.

Laying the foundations for a secure quantum future

Becoming secure in the post-quantum world requires the implementation of quantum-secure technologies, scaled to the needs of the organization.

In addition to understanding the technical elements that underpin quantum resilience, organizations also need to view their critical assets and processes through a risk-based lens, in order to make appropriate investment decisions.

Become crypto-agile

Ensure your environment is crypto-agile, i.e., able to work with longer keys, and able to replace old encryption algorithms with new quantum-resistant encryption algorithms (QRA) recommended by NIST.[4]

Implement full-entropy random numbers

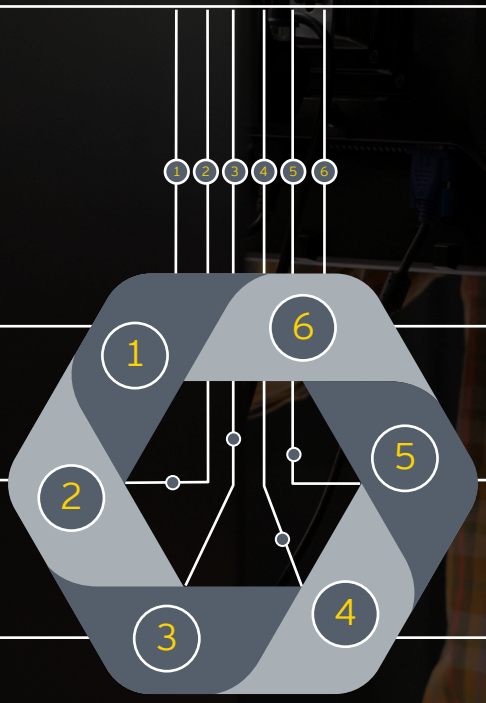
Use full-entropy random numbers. These are necessary for quantum-resilient cryptography.[4]

Use longer keys for symmetric encryption

Symmetric encryption keys will need to be twice as long as those used today to enable similar protection, due to quantum computing speeding up brute force attacks and halving effective key lengths.[4]

Deploy Quantum Key Distribution

Explore key exchange solutions such as quantum key-distribution (QKD). Use secure links between key management nodes, protected by QKD and quantum-resistant algorithms.[4]



Identification
Identification of IT assets where potentially vulnerable cryptography is used

Business scenarios
Mapping of crypto-enabled IT assets to business processes and then to client experience scenarios

Risk picture
Development of the overarching and holistic risk picture on technical, operational, client and socio levels with links between risk levels

Implementation
Implementation of the end-to-end roadmap and update of risk scenarios over time as quantum technology evolves

Quantum resilience
Development of a quantum resilience plan covering technical, operational and client aspects based on the chosen risk appetite

Risk scenarios
Risk and cost/benefit analysis for possible scenarios meeting different levels of risk appetite

[4] https://www.quintessencelabs.com/quantum-safe-cyber-security/

Contacts

Jeremy Pizzala

EY Asia-Pacific
Cybersecurity Leader

Rohit Rao

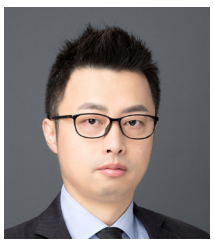
EY Asia-Pacific Financial Services
Cybersecurity Leader

Steve Lam

Partner, Cybersecurity
Ernst & Young Advisory Pte. Ltd.

Naoshi Matsushita

Partner, Cybersecurity
Ernst & Young Business Partner
Co., Ltd.



Kelvin Gao

Partner, Cybersecurity
Ernst & Young (China) Advisory Ltd.

Sang Woo Kim

Partner, Cybersecurity
EY Consulting LLC.

Alexey Bocharnikov

EY Asia-Pacific
Quantum Technology leader

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 000325-23Gbl

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com