Quantum Computing Puts Cryptography Under Pressure

Why Boards Must Re-Examine Long Term Data Protection

量子運算使加密技術受壓

為何董事會有必要重新審視對數據的長期保護

Edwin Bernard

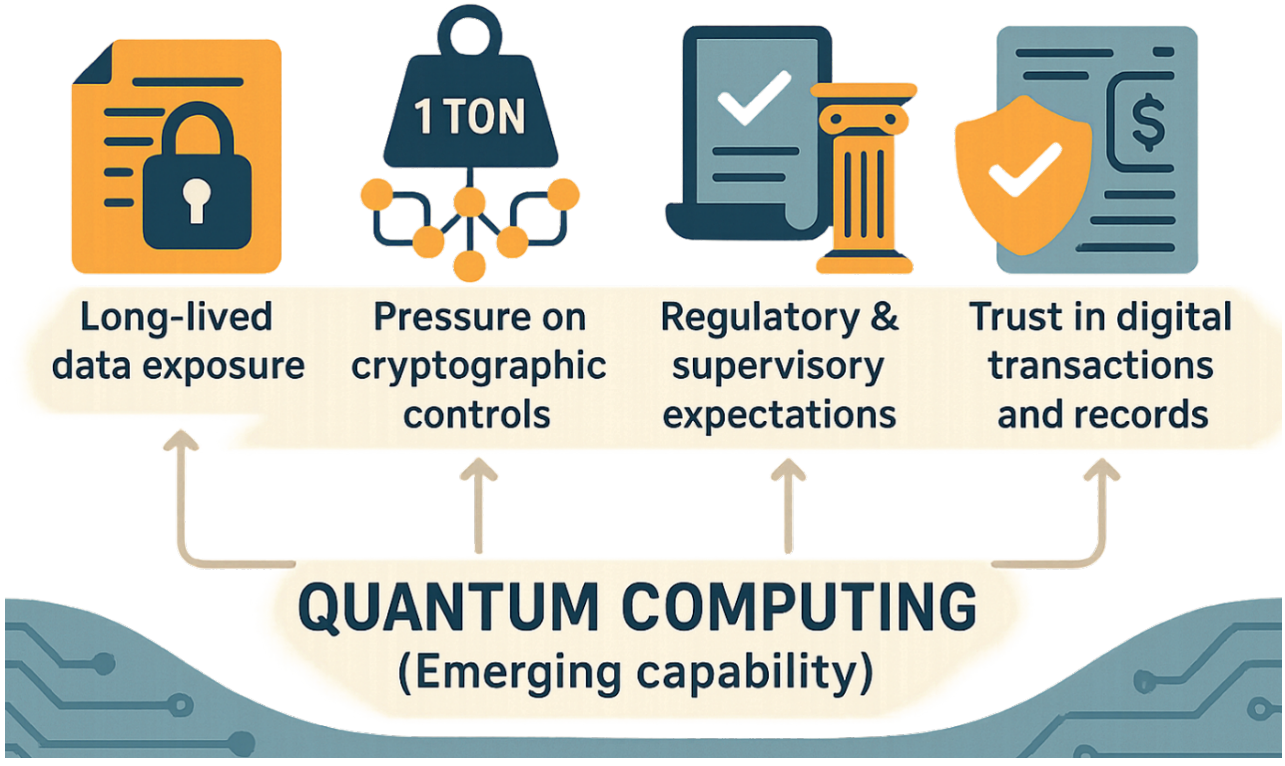
Quantum computing has moved steadily from scientific discussion into regulatory and governance conversations. While still an emerging technology, it is increasingly referenced in the context of cybersecurity, data protection, and long term institutional resilience. This matters. When regulators begin to acknowledge a risk, directors are expected to take notice—not because immediate action is required, but because the issue has crossed the threshold of foreseeability.

For Hong Kong boards, quantum computing is not a technology to be deployed, nor a capability most organisations are expected to build. Its relevance lies in what it challenges: long standing assumptions about cryptography, which underpins digital trust, data security, and the integrity of modern business operations. As with artificial intelligence, the governance challenge is not technical mastery, but judgment.

This article considers quantum computing from a boardroom perspective. It does not predict technological timelines or advocate early adoption. Instead, it focuses on why boards should re examine how long term data protection is governed as cryptographic assumptions come under increasing pressure.

What Quantum Computing Is—and What It Is Not

Quantum computing is often misunderstood as simply a faster version of today's computers. This is not the case. It does not represent general speed improvements or incremental efficiency gains. Instead, it is a different approach to computation that, for certain categories of problems, may eventually enable outcomes that classical computing cannot achieve at all.



For directors, this distinction is important. The governance relevance of quantum computing does not lie in performance or productivity, but in its potential to challenge foundational assumptions—particularly those relating to cryptography. Much of today's digital security relies on encryption methods that are considered robust against existing computing techniques. Over time, advances in computational capability could place pressure on those assurances.

It is this pressure on foundational controls, rather than "faster computing," that brings quantum computing into the governance conversation.

Why Cryptography Has Become a Board Level Concern

Cybersecurity has evolved from an operational matter into a core enterprise risk issue. Data breaches, fraud, and system failures now carry legal, financial, and reputational consequences. Regulators increasingly expect boards to exercise meaningful oversight, not merely to receive assurance after incidents occur.

Quantum computing enters this discussion because it affects cryptography—the mechanism that protects data, transactions, and trust. While existing encryption remains effective today, its potential need to evolve over time changes how boards should think about long term data protection.

This is particularly relevant for organisations that hold sensitive data over extended periods, including customer information, financial records, and intellectual property. A widely discussed concern is that encrypted data collected today could be retained and decrypted in the future once computational techniques mature. This "harvest now, decrypt later" dynamic does not imply imminent exposure, but it does challenge boards to consider whether present day controls remain appropriate for long lived risk.

While some historically harvested data may already be exposed to future decryption, the board's present responsibility lies in preventing the continued expansion of that exposure by strengthening protections for data whose value and sensitivity extend well into the future.

Regulatory Signals and the Expectation of Foresight

In Hong Kong, quantum-related risk is emerging through regulatory signalling rather than prescriptive requirements. A notable recent development is the Hong Kong Monetary Authority's (HKMA) announcement of a Quantum Preparedness Index to assess the banking sector's readiness for Post-Quantum Cryptography (PQC). The initiative reflects growing supervisory recognition that cryptographic resilience is becoming a long-horizon governance issue.

For organisations outside financial services, this does not create a present-day legal obligation; rather, it functions as a regulatory barometer, signalling how supervisors are beginning to frame expectations around long-term cryptographic resilience. It does, however, serve as an indicator of regulatory awareness. When supervisors begin assessing preparedness—rather than responding only to incidents—directors elsewhere should consider whether their own oversight remains sufficiently forward-looking.

In a principles based regulatory environment, such signals are often more instructive than formal rules.

A Practical Governance Lens for Quantum Risk

For boards seeking to translate quantum related uncertainty into practical oversight, three governance lenses are particularly useful.

Data longevity

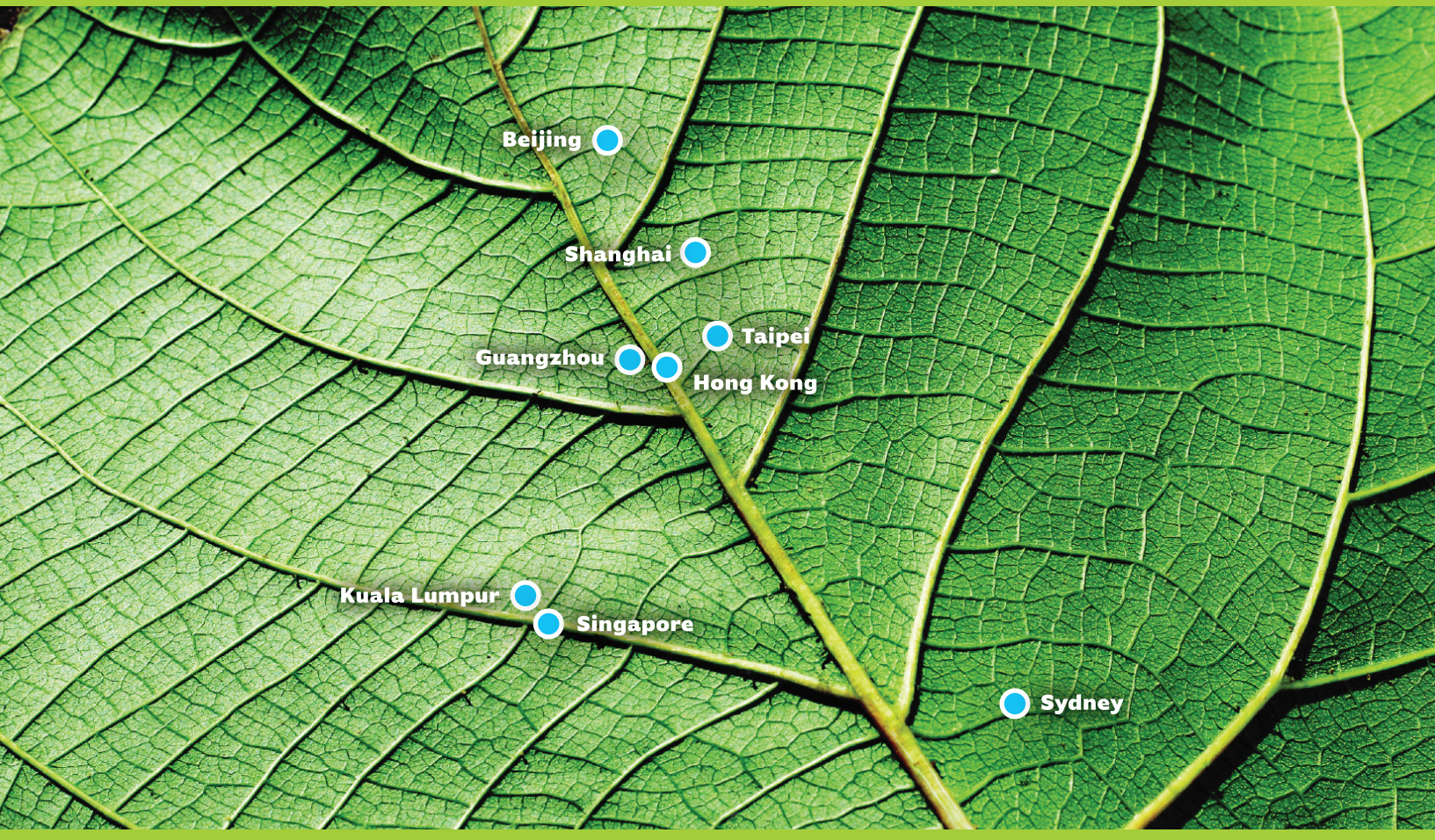
The governance challenge is not how data is encrypted today, but how long sensitive data retains value and exposure. Boards should satisfy themselves that management understands which datasets must remain secure for many years—or decades—and how data retention practices interact with evolving security assumptions. This is a question of asset stewardship and risk horizon, rather than encryption design.

Dependency mapping

Few organisations control their cryptographic environment end-to-end. Critical dependencies often sit with cloud providers, software vendors, and outsourced infrastructure. In practice, achieving such adaptability is often constrained less by cryptographic choice than by architectural complexity, including deep dependencies on cloud platforms, software vendors, and long-lived legacy systems. Boards should therefore consider where these dependencies lie and how easily they could adapt if cryptographic standards evolve. This mirrors familiar governance concerns around supplier concentration and operational resilience, applied to digital trust.

Regulatory alignment

In Hong Kong's principles based system, boards are not evaluated solely on technical compliance, but on the reasonableness of their judgment. Initiatives such as the HKMA's Quantum Preparedness Index, alongside broader digital policy coordination through the Digital Policy Office,



Shared Roots. Shared Aspirations.

From every branch, we deliver expertise that is trusted and globally recognised.

PRovoke Media

20 Best Financial PR Agencies in the World

100 Best Corporate PR Agencies in the World

30 Best Healthcare PR Agencies in the World

100 Best PR Agencies in the World

PR NEWS

Elite Top **120** by PRNEWS Agency

Asia-Pacific Stevie® Awards

APAC PACIFIC STEVIE AWARDS 2026
1 SILVER

APAC PACIFIC STEVIE AWARDS 2026
2 BRONZE

PR Awards Asia Pacific 2026

GOLD PR Awards Asia Pacific 2026

www.sprg.asia

SPRG STRATEGIC PUBLIC RELATIONS GROUP 縱橫公共關係顧問集團

Hong Kong ◆ Beijing ◆ Shanghai ◆ Guangzhou ◆ Taipei ◆ Singapore ◆ Kuala Lumpur ◆ Sydney

signal growing regulatory awareness of long-term cryptographic resilience. Boards should ensure their oversight reflects this context and can be explained coherently if questioned in the future.

Taken together, these lenses do not require boards to forecast technological timelines. They simply help directors govern what is already foreseeable.

Crypto Agility as a Board Level Objective

From a governance perspective, the constructive response to quantum-related uncertainty is not premature technological change, but crypto-agility. Crypto-agility refers to the organisation's ability to evolve its cryptographic controls over time without undermining operations, compliance, or stakeholder trust.

This is a governance capability rather than a technical project. From a board perspective, crypto-agility is not about an immediate or wholesale replacement of systems. It is a phased, risk-based investment approach that recognises both the cost of change and the cost of inflexibility, and seeks to preserve operational and strategic options over time.

Boards already think in similar terms when overseeing supply-chain resilience, capital flexibility, or succession planning. Crypto-agility extends this mindset to digital security. The relevant board-level question is not whether today's encryption is adequate, but whether the organisation is positioned to adapt smoothly when assumptions change.

Governance Context and Common Pitfalls

Hong Kong's governance framework places emphasis on discretion and accountability. There is no quantum specific regulation. Instead, expectations are developing through guidance, supervisory practice, and policy alignment. In such an environment, the absence of explicit rules does not imply the absence of responsibility.

Boards should also avoid two common pitfalls. The first is complacency—assuming that because quantum disruption is not imminent, it can be ignored. The second is overreaction—responding to early signals with premature or symbolic technical commitments. Sound governance lies between these extremes, focusing on preparedness rather than speculation.

Conclusion

Quantum computing does not eliminate encryption, nor does it render existing cryptography obsolete. It does, however, place increasing pressure on long standing security assumptions that underpin long term data protection.

For boards, the challenge is not technological, but governance related. As regulatory awareness grows, directors will be assessed not on technical expertise, but on whether they exercised informed oversight when the implications became foreseeable.

In Hong Kong's principles based framework, this calls for judgment rather than prediction. Quantum computing therefore serves as a test of governance maturity—how boards respond when certainty has yet to arrive, but responsibility already has.

Edwin Bernard, MSc, CEFA, CAITL (Certified Artificial Intelligence Transformation Leader, USAII)

量子運算已漸漸由科學研討議題成為規管和公司管治議題。雖然量子運算依然是新興科技，但在網絡安全、數據保護和企業長遠韌性方面亦日益備受談論，因此不容忽視。每當規管當局開始認為出現了一種風險，董事必須加以注意，這不是因為有必要即時採取行動，而是因為該事宜已是可以預見。

量子運算對香港的董事會來說不是必須部署的科技，也不是大部分企業應該打造的能力，量子運算之所以不容忽視，是因為它對加密技術的固有假設構成挑戰，而數碼信任、數據安全和現代商業營運的完整性均依賴這些假設。跟人工智能一樣，公司管治面臨的挑戰並非在於必須精通這種科技，而是在於判斷力。

本文將從董事會的角度探討量子運算，本文不會預測科技發展進程或鼓勵及早應用量子運算，而是集中討論在現有加密技術的安全假設日益受到挑戰的情況下，董事會必須重新審視數據長期保護的管理。

何謂量子運算

量子運算常被誤解為只不過是當今電腦的快速版本。事實並非如此。量子運算不是旨在加快整體速度或提高增量效益，它是一種不同的運算方式，最終可就某類問題提出傳統運算法根本無法得出的結果。

對董事來說，這種區別十分重要。量子運算對公司管治的重要性不在於業績或產能，而是其挑戰基本假設的潛能 — 特別是對加密技術的假設。現時，數碼安全主要依賴加密法，加密法被視為能夠應付現有的電腦技術，假以時日當運算力更加先進，加密法可能無法做到萬無一失因而受壓。

量子運算之所以成為公司管治的議題，正是因為它對基本控制構成壓力，而非因為其「運算力更快」。

為什麼加密技術成為董事會層面的關注

網絡安全已從營運攸關變成企業的核心風險。現在，數據洩漏、欺詐和系統失靈都會帶來法律、財務和聲譽後果。規管當局日益期望董事會執行有效監管，而非在事後作出保證。

是次研討提及量子運算，是因為量子運算影響加密技術這種針對數據、交易和信任的保護機制。雖然現有的加密法至今奏效，但有鑑於加密法可能有需要隨著時間蛻變，董事會必須考量採取別的方法來長期保護數據。

對於長時間持有客戶資訊、財務紀錄和知識產權等敏感數據的企業來說，這點尤其重要。一項廣受討論的關注是今天收集到的資料雖被加密，在未來一旦運算技術趨成熟有可能被保留和解密。雖然這種「先收集、後解密」的情況不會即時構成風險，但董事的確因此而需要檢討現時的管控措施是否適用於長久不散的風險。

雖然一些在過去收集得的數據現在可能已遭受到未來解密，但董事會目前的責任是加強保護一些在未來仍有價值和敏感的數據，以防止這種未來解密的情況蔓延。

規管當局發放信號及預期未雨綢繆

量子相關風險正在香港冒起，但規管當局只是發出信號而非規定性要求，最明顯可見如香港金融管理局最近宣佈推出「量子準備度指數」，以評估銀行業在後量子加密技術（PQC）領域的準備情況。此舉反映規管當局日益認同加密韌性是公司管治的長遠事務。

這只是一種規管量計，並不對非金融服務企業產生即時法律責任，顯示出監督者開始期待企業具備長遠加密韌性。但是，此舉確實反映規管當局對這方面的意識。當監督者開始評估企業的準備度（並非因任何事件作出的回應），其他企業的董事應該考慮本身的監管是否充分未雨綢繆。

在原則為本的規管環境下，這類信號往往是指示性質而非正式規條。

量子風險務實管治鏡

對力求將量子不確定性化作務實監管的董事會來說，以下三面管治鏡尤其有幫助：

數據壽命

公司管治面對的挑戰不是當下如何加密數據，而是敏感數據的價值和風險會維持多久。董事會必須確定管理層知道哪些數據集必須保持安全數年甚或數十年，以及數據保存措施如何因應保安假設轉變而轉變。這點關乎資產盡職治理和風險期，而非加密設計。

審查依賴性

很少企業以端對端的方式控制其加密環境。關鍵往往是依賴雲端計算服務供應商、軟件供應商和外判基礎設施。實際上，企業能否靈活應對未來加密技術的變化，所面對的限制往往並非來自所採用的加密演算法，而是源於整體系統架構的複雜性，這是指高度依賴雲端計算平台、軟件供應商和長期運行的舊有系統。因此，董事會必須審視關鍵依賴關係所在，以及一旦加密標準轉變可以如何輕易適應。這顯示公司管治對數碼信任的關注程度媲美對供應商集中度和營運韌性的關注程度。

配合規管

在香港的原則為本規管制度下，董事會並非單單根據技術合規接受評估，而是根據所作的判斷是否合理。金管局的「量子準備度指數」一類措施和透過數字政策辦公室執行的整體數碼政策統籌顯示規管當局越來越注意加密的長遠韌性。董事會必須確保其監管切合這點，在日後一旦受查問時能夠圓滿解釋。

總的來說，這三面鏡並非要求董事會預測技術時間線，只是協助董事管治已經可預見的事宜。

加密敏捷性是董事會層面的目標

從公司管治的角度來說，正面應對量子相關不確定性並非預早作出技術轉變，而是建立加密敏捷性。加密敏捷性是指企業有能力隨著時間改變其加密管控但不削弱營運、合規或股東信任。

這點關乎公司管治能力而非技術項目。從董事會的角度來看，加密敏捷性並非指即時或全盤取締系統，而是一種認同變動成本和欠缺靈活代價的風險為本分期投資，目的是假以時日保存營運和策略選項。

董事會在監督供應鏈韌性、資本靈活性或繼任計劃時採用的思維也是這樣，加密敏捷性將這種思維延伸至數碼安全。在這方面，董事會層面的問題不是當今的加密法是否足夠，而是當假設改變時企業本身是否有能力順利適應。

管治與陷阱

香港的公司管治框架著重酌情權和問責性，並無特別規管量子事宜，這方面的預期只是透過指引、監督措施和政策配合衍生。有鑑於此，沒有明文規則並不意味著沒有責任。

另外，董事會必須規避兩個常見的陷阱。第一個陷阱是固步自封，即是假設量子顛覆不會在短期內出現，故此置之不理。第二個陷阱是反應過度，即是一出現早期跡象便過早承諾或作出象徵式技術承諾。卓越的公司管治介乎這兩個極端之間，專注於作好準備而不是一味猜測。

結論

量子運算不會淘汰加密法，也不會令現有的加密技術遭廢棄，但會為支援數據長期保護的固有保安假設增添壓力。

對董事會來說，這項挑戰不是技術性挑戰而是跟公司管治攸關。隨著規管當局的意識加強，董事不會根據技術專業能力接受評估，而是根據當影響變得可以預見時有否執行知情監管。

在香港的原則為本框架下，判斷力較預測更重要。因此，量子運算可測驗公司管治的成熟度，即是當不確定性尚未實現但須肩負相關責任時，董事會如何應對。

Edwin Bernard（理學碩士、歐洲認可金融分析師、美國人工智能學會認可人工智能革新領袖）

The 21st Century DIRECTOR 廿一世紀董事

Publisher 出版機構
The Hong Kong Institute of Directors 香港董事學會

Sponsor 贊助機構
Corporate Governance Development Foundation Fund 企業管治發展基金

Project Management 項目統籌
Secretariat, The Hong Kong Institute of Directors
香港董事學會祕書處

For enquiries about circulation and advertisement, please contact:
有關發行及廣告查詢，請聯絡：
Chief Business Officer & Head of Training: Ms Miriam Yee
業務總監及培訓主管：余海恩小姐

For editorial enquiries, please contact:
有關編輯上的查詢，請聯絡：
Associate Manager, Communication & Projects: Mr Wing Wong
傳訊及項目助理經理：王俊泳先生

Tel 電話： +852 2889 1414
Fax 傳真： +852 2889 9982
Email 電郵： magazine@hkiod.com

《廿一世紀董事》同時可於網上閱覽
The 21st Century Director is also available at
https://www.hkiod.com/21st-century/

ISSN 1996-9619

Sponsored by 贊助機構：
Corporate Governance
Development Foundation Fund
企業管治發展基金

The Hong Kong Institute of Directors is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors.
香港董事學會為香港代表專業董事的首要組織，其宗旨是促進所有公司的持久成就；為達成使命，學會致力提倡優秀企業管治與釐訂相關標準，以及協助董事的專業發展。

The Hong Kong Institute of Directors Executive Office 香港董事學會行政處
2104 Shanghai Industrial Investment Building, 48 Hennessy Road, Wan Chai, Hong Kong 香港灣仔軒尼詩道48號上海實業大廈2104
Tel 電話 : (852) 2889 9986 Fax 傳真 : (852) 2889 9982 E-mail 電郵 : executive@hkiod.com