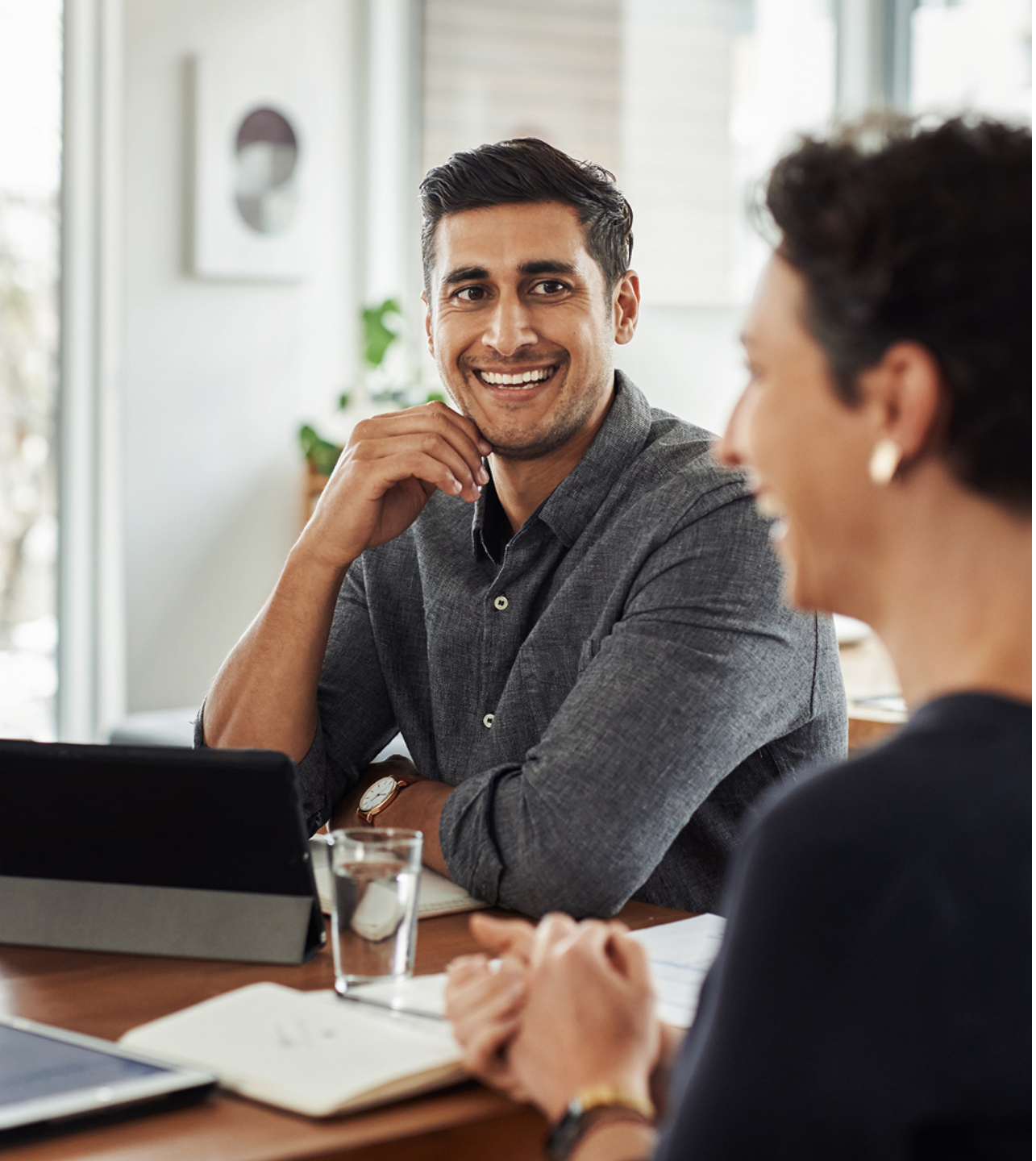
CIO

Expert Exchange

Q1 Executive summary
March 25, 2026

kyndryl



Overview

The recent roundtable exchange brought together technology leaders across various industries discussing business resiliency across accountability, third-party risk, cloud strategy, and data sovereignty amid geopolitical uncertainty. While no single risk-ownership model stood out, participants agreed resiliency hinges more on clear accountability, board visibility, and sustained investment than on reporting structures. Discussion highlighted pressures from vendor concentration, cloud and SaaS lock-in, supply constraints, and rising costs, driving a shift from “cloud first” to “cloud smart” approaches such as selective repatriation, multi-cloud strategies, and stronger FinOps. Leaders also noted rising Canadian data residency requirements, tighter hyperscaler contracts, and renewed interest in domestic capabilities, while recognizing the limits of full sovereignty in productivity platforms, AI, and global supply chains.

Host(s)

Karen Cheng
CTO, Kyndryl Canada

Brian Medeiros
President, Kyndryl Canada

Key topics

Organizational structures of risk and security accountability

- Organizations take various approaches to whether technology operations and cybersecurity risk should be centralized under a single leader or separated to maintain independent oversight and avoid conflicts of interest.

- Some leaders advocate combining technology infrastructure and security functions into a single role reporting directly to the board of directors. They argue this consolidated structure creates valuable operational synergies and allows the organization to make focused, long-term investments in building a highly secure operating environment.

- Others prefer separating the chief information officer and chief information security officer roles into distinct reporting lines. Separating these functions creates a structural check and balance that keeps both sides honest, ensuring that security leaders do not end up auditing their own operational work.

- Leaders operating in highly regulated environments often rely on a distributed risk management model in which business risk resides with operational, risk, or legal teams. In these decentralized models, maintaining close collaboration between security and operational departments is essential to present a unified risk profile to oversight committees.

- Regardless of the reporting structure, infrastructure teams repeatedly bear the operational and financial burden of executing sudden, mandatory security upgrades. A common friction point involves security teams raising urgent vulnerabilities without providing the necessary funding, highlighting a critical best practice to systematically budget money and staff capacity for unplannable risks.

> **"There is an inherent tension between combining operational and security teams to deliver services faster versus splitting them apart to create a necessary check-and-balance relationship."**
>
> — CIO Expert Exchange Member

Evolving data hosting strategies and data sovereignty

- Organizations are transitioning from the automatic adoption of external data hosting toward highly selective deployments driven by cost containment, infrastructure rightsizing and strict national data sovereignty requirements.

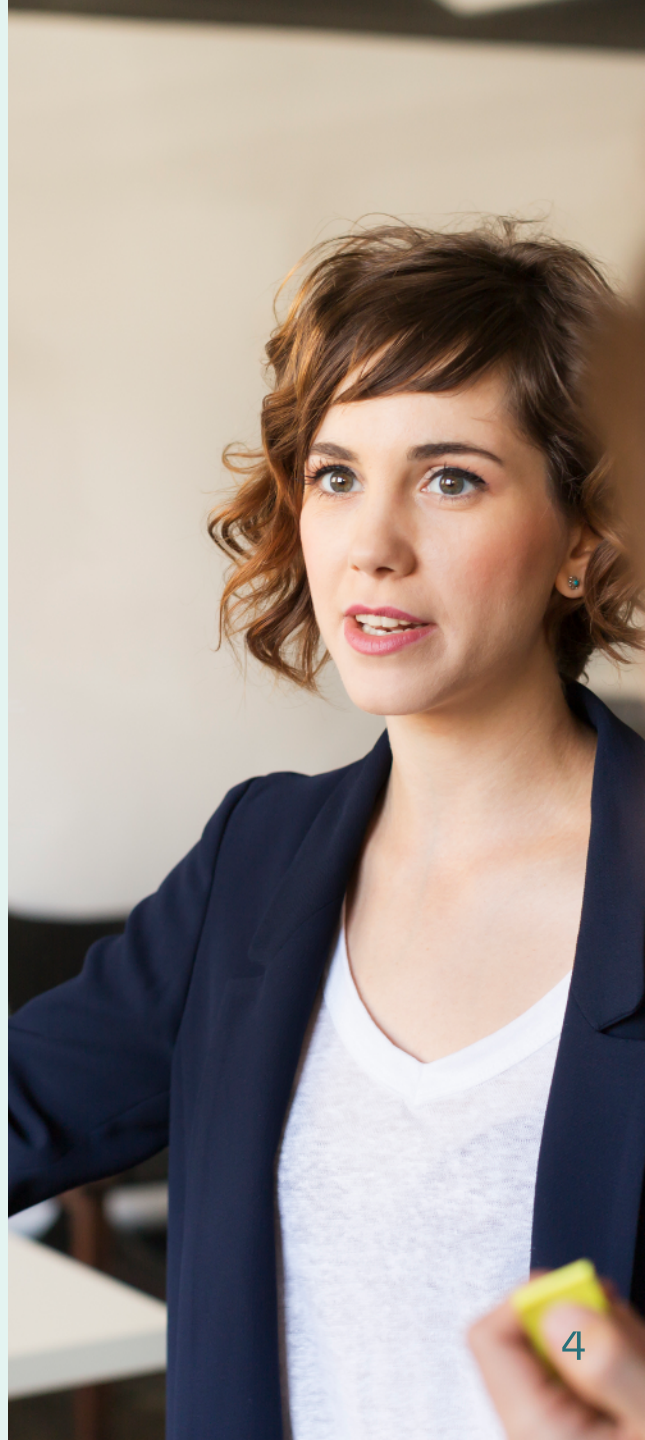
- Members shared that mandates to move all systems and workloads to the cloud are being replaced by more nuanced, mixed hosting environments. Many leaders noted that migrating legacy computing workloads without modernizing them often increases overall costs, prompting them to actively evaluate which systems should remain in internal data centers.

- Geopolitical tensions are forcing businesses to enforce strict geographical boundaries on their sensitive information. Executives shared that they now mandate that their systems and highly sensitive workloads reside strictly within national borders, and they increasingly require contracts to be signed exclusively with local vendor affiliates.

- Due to escalating consumption costs, several organizations are building FinOps models to justify bringing specific technology workloads back into their own facilities. Leaders are carefully balancing the flexibility of external platforms against long-term operational costs, electricity usage and the loss of direct control over their physical digital environments.

- To maximize the financial benefit of external hosting, technology leaders emphasized the absolute necessity of actively managing infrastructure size. They highlighted that cost savings only materialize when financial operations teams rigorously monitor consumption and automatically turn off unused testing or development environments outside of normal working hours.

> "We are actively shifting away from a rigid strategy that prioritizes external hosting first, because paying for continuous consumption is becoming increasingly expensive and exposes our data to global geopolitical vulnerabilities."
>
> — CIO Expert Exchange Member



Mitigating supply chain vulnerabilities and vendor dependence

- Severe hardware shortages and aggressive software pricing models are driving business leaders to reconsider single-vendor strategies and explore innovative methods to extend the lifespan of existing corporate assets.

- Executives expressed frustration with major hardware suppliers who lack long-term supply strategies amidst global manufacturing shortages. Participants noted that vendors frequently respond to supply constraints simply by raising prices and advising clients to hoard equipment, leaving organizations struggling to effectively plan their standard hardware replacement cycles.

- To combat rising equipment replacement costs, infrastructure teams are deploying advanced monitoring software to measure the actual health, battery life, and processing performance of devices. By utilizing this real-time data, organizations can safely delay replacing healthy machines and also reclaim unused software licenses, thereby reducing their immediate capital expenditures.

- While historically aggregating purchases has driven down costs, leaders warned that over-consolidation has introduced dangerous single points of failure. Members noted past experiences in which reliance on a single supplier caused critical operational disruptions, prompting a deliberate shift toward maintaining active contracts with multiple competing vendors.

- By directing enterprise purchasing power toward domestic businesses, leaders aim to stimulate the growth of local artificial intelligence innovations. Participants acknowledged that while these investments take years to show dividends, they remain crucial for building a competitive national technology sector over the next decade.

- To further reduce dependency on expensive commercial software, several organizations are adopting free, independent software frameworks for non-critical operations. Leaders noted that teams successfully utilize these open source solutions to perform data visualization and internal dashboard creation, reducing overall software licensing costs. Executives agreed that deploying these unmanaged tools requires extreme caution, strict quality control and dedicated internal staff to provide ongoing maintenance and security support.

> “The operational efficiencies and financial benefits of adopting a single technology provider must now be carefully weighed against the severe risk that permanent vendor lock-in creates.”
>
> — CIO Expert Exchange Member

kyndryl

To learn more about the Kyndryl Canada CIO Expert Exchange or to become a member of this community, please visit this website.