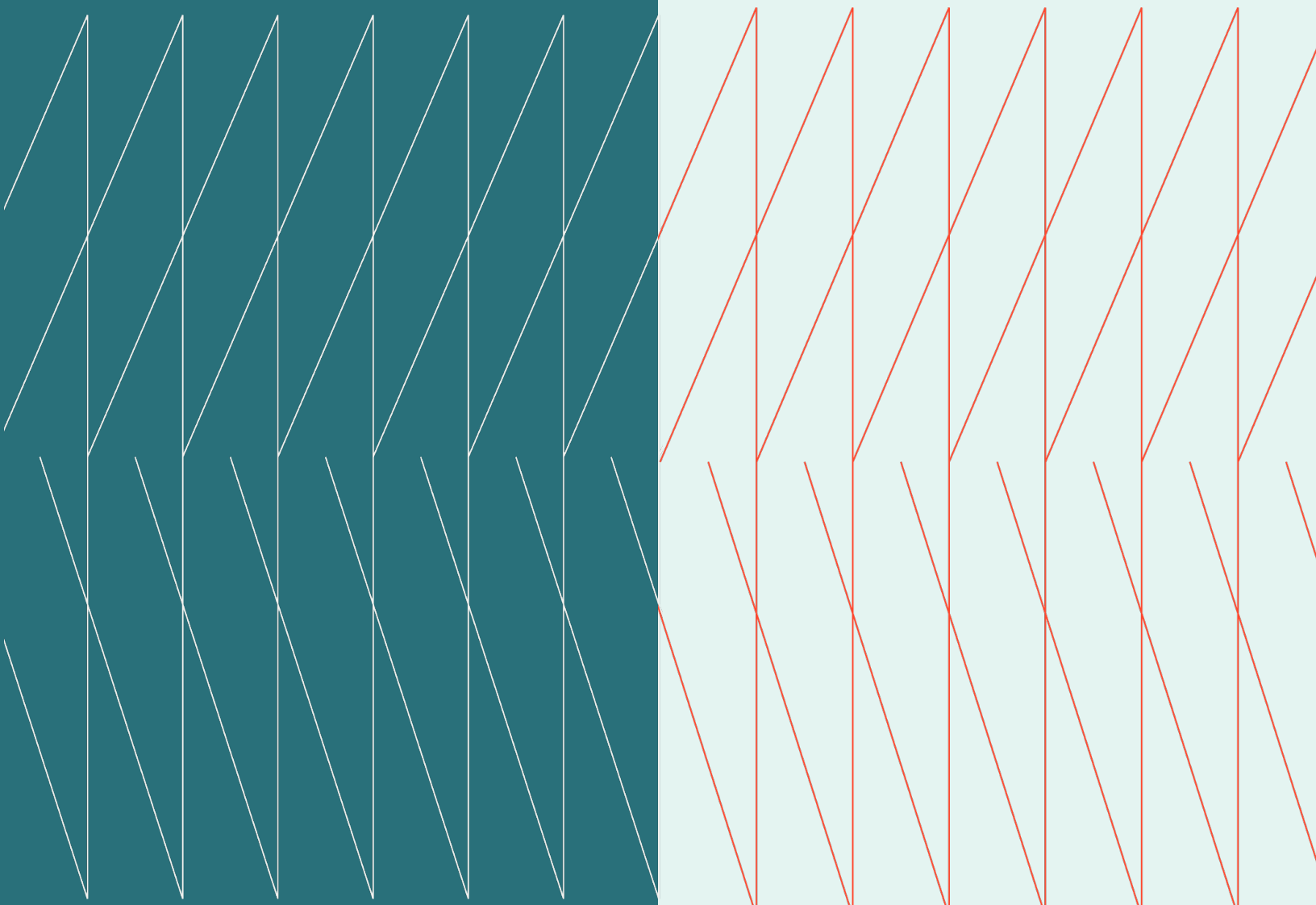
CIO

Expert Exchange

February 25, 2025

kyndryl

Executive Summary



Hosts:

Farhaz Thobani
President, Kyndryl Canada

Stewart Hyman
Chief Technology Officer, Kyndryl Canada

Overview

In this Expert Exchange session, the CIO community convened to discuss the topics below. The agenda was determined based on mutual interest through advance interviews with participants.

Expert Exchange themes

- Tariffs and Economic Uncertainty
- Data Sovereignty
- Mitigating Risks
- Cyber Security and Deepfakes

Tariffs and Economic Uncertainty

- CIOs and their organizations are keeping a close eye on the US as it continues to push forward with enacting tariffs. Given the high level of uncertainty around whether tariffs will come to pass and what rate they might be, most organizations are adopting a wait-and-see approach as things unfold.

- Even if tariffs don't directly impact an organization's business, everyone will still feel economic effects. Currency fluctuations and increased service fees on specific products are likely. Perhaps more relevant to CIOs are concerns about higher service costs from cloud and SAAS providers (in other words, higher hardware costs due to tariffs could result in increased service pricing). Members agreed that tariffs would dramatically impact the hardware supply chain.

- Some leaders see US tariff threats as an opportunity rather than a challenge. They see the threat as an opportunity to revisit their "laziness" in leveraging US companies rather than investing in and building a Canadian ecosystem. Tariffs could be the wake-up call organizations need to develop capabilities themselves.

- "Sometimes something crosses the border with Mexico and the border with the US three or four times before it makes its way to Canada, and that's going to be hit by tariffs every single time it crosses a border. So, there are many different ways these tariffs could effectively hit us." – Kyndryl Canada Cross-Industry CIO Expert Exchange Member.

Data Sovereignty

- Similar to tariffs, fears around data could push companies to invest in the infrastructure necessary to keep data safe and secure in Canada—one CIO envisioned Canada becoming the "Switzerland bank" of data worldwide. This push to become a global leader in data security could be especially necessary if Canada begins to feel it is no longer in lockstep with the US on issues such as data sovereignty and security.

- A member noted that it's crucial to establish data sovereignty and residency upfront because it is hard to backtrack once data is already being shared across industries and borders. It's challenging (but necessary) to establish among institutions that share heavily (for example, universities) and when using hyperscalers with global footprints.

- "I would love to get to a place where Canada became the Switzerland of databanks, where people would look to Canadian companies and be sure that their data is safe when it's residing in Canada... There's all sorts of opportunity." – Kyndryl Canada Cross-Industry CIO Expert Exchange Member.

- "I'm most concerned about the sovereignty and data residency because it's tough to return to that. We, of course, prefer our data stored in Canada, but so many of these SAAS providers have a global service component, which you just can't work around." – Kyndryl Canada Cross-Industry CIO Expert Exchange Member.

Mitigating Risks

- While tariffs have an immediate cost risk, there is also a long-term risk that if tariffs become too pervasive or prohibitive, certain supply chains will "dry up" (for example, China will start redirecting some of its components to other markets). With many organizations not positioned to source necessary hardware from different jurisdictions, they must take steps now to mitigate long-term risks and be able to pivot to new suppliers.

- From a technology perspective, there is a lot of uncertainty in the environment. Even as they wait for clarity, organizations must have a business continuity plan to know where they have risks, where they can move to an outsourced model, where they can host in-country, and where to create continuity plans.

- Organizations are looking harder at contracts, especially those up for renewal, to ensure they mitigate any tariff-related risks. CIOs noted renewal increases are no longer the traditional 3% annually, but sometimes 10-20% with no caps on increases, even on multi-year contracts. While large organizations and government institutions can absorb this, the budgets of smaller companies simply cannot. This vendor pricing mindset is driven by inflationary pressures, fears of future inflationary pressures, and vendor lock-in, where vendors have unique products that customers can't really escape from.

- Price certainty should be the focus of any contract negotiation in the short term. Depending on the degree of price certainty, a company can then weigh those increased costs against the costs of transitioning to a competing vendor.

- One member suggested doing early RFPs as a way of mitigating some risks around renewals. Rather than waiting until six months before renewal to start negotiating, sending out RFPs well in advance gives an organization time to perform a better business analysis and gauge any alternatives.

- "The big ones are more problematic than the smaller stuff that we're dealing with. You could probably find another laptop provider versus the bigger software products that anchor our stores today." – Kyndryl Canada Cross-Industry CIO Expert Exchange Member

Cyber Security and Deepfakes

- Resiliency plans go beyond economic risks and cost pressures, with many CIOs noting the ever-increasing cyber security threats they face. In addition to ransomware and phishing, deepfake video and audio impersonating high-level leaders are becoming harder to identify, raising the risk of attacks using false instructions or authentication.

- Deepfakes pose a growing threat, prompting companies to implement security training around the topic. Examples included showing deepfake videos to the board and calling EVPs with a deepfake CEO voice. While technologies are emerging to combat deepfakes, like all cyber security, training remains the best defense.

- While AI can help strengthen security, it is also being used to augment cyber-attacks. AI-driven phishing emails with realistic company logos have higher click rates, even among trained users. Tracking clicks, detecting suspicious emails, and reporting them help defend against these advanced threats.

- "I am not getting any traction and getting a lot of pushback from my board around doing a deepfake test, particularly involving a CEO or CFO. So, I think there is a lack of understanding of the risk across that level of the organization. But this is a reality that is happening." – Kyndryl Canada Cross-Industry CIO Expert Exchange Member.

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

kyndryl