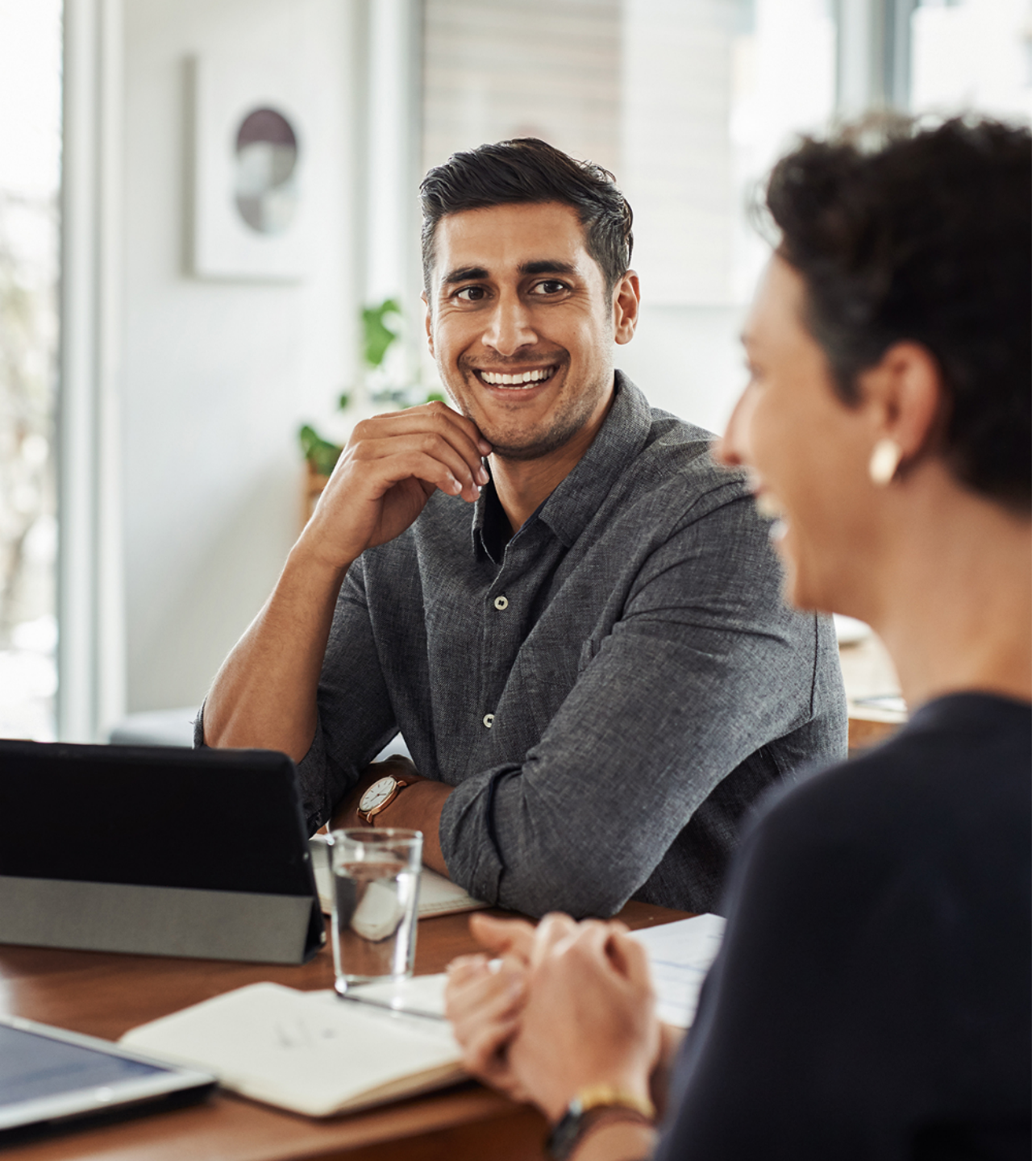
Canada CISO

Expert Exchange

Frontier AI Cyber Resilience
April 22, 2026

kyndryl



Overview

Senior cybersecurity and technology leaders met to discuss AI-era operating readiness, focusing on how AI-driven vulnerability discovery is compressing the window between discovery and exploitation and exposing the limits of legacy cyber models. Key themes included the breakdown of traditional vulnerability management, the need to balance prevention with resilience, and the difficulty of governing rapid, uncertain change.

Host

Denis Villeneuve
Kyndryl, Canada Cyber Resilience and Connectivity Practice Leader

SME

Cory Musselman
Kyndryl, Global Chief Information Security Officer

Key topics

The Collapse of Traditional Vulnerability Management

- There is an erosion of long-standing assumptions underpinning vulnerability management. AI-enabled models are now capable of rapidly identifying, chaining, and operationalizing vulnerabilities across vendors and technologies. This shift renders traditional patch prioritization models, backlog tolerance, and compliance-driven metrics insufficient. As a result, vulnerability backlogs are no longer viewed as technical debt but as active and compounding operational risk.

- The tension between discovery and remediation speed is a top-of-mind challenge for security leaders. While organizations have historically relied on predictable patch cycles and change windows, AI-driven exploitation compresses response timelines beyond what existing governance structures can accommodate. This creates an environment where even well-run programs struggle to keep pace. The implication is a forced rethinking of what "acceptable exposure" means in practice.

- Many security and resiliency operating models have long recognized the existence of zero-day vulnerabilities and the reality that patches are not always immediately available. What has changed materially is the compression of the time between vulnerability discovery and exploitation. Historically, even when zero-days existed, organizations often benefited from a longer mean time to exploit once a vulnerability became known, allowing time to assess risk and apply patches when they were released. As that window continues to shrink, organizations are increasingly compelled to rely on compensating controls, isolation, and resilience measures alongside traditional patching. This shift introduces more acute tradeoffs between availability, performance, and risk containment.

- There is a growing recognition that vulnerability management is shifting from a discrete security function to a continuous operational discipline. This evolution places new demands on asset visibility, exposure management, and real-time decision-making. However, accelerating response without increasing fragility remains a core challenge. Leaders have acknowledged that speed without control can create its own form of systemic risk.

"The expectation is that time to exploit will drop into hours instead of days, weeks, or months — and that's something we haven't dealt with before."

— Cory Musselman,
Global CISO, Kyndryl

Outpacing risk: Security readiness for the AI era

Learn more

Operating Model Strain and the Limits of Process

- There is inherent tension between existing IT and security processes and the need for rapid, high-confidence action. Manual change controls, ticketing workflows, and approval boards are identified as bottlenecks under AI-driven threat conditions. While these controls were designed to reduce risk, they now risk becoming sources of delay. This forces organizations to reconsider which safeguards remain fit for purpose.

- An emerging pattern across organizations is the creation of temporary war rooms to bypass traditional decision paths. These constructs bring together security, IT, business, and risk leaders to make time-sensitive decisions in the face of uncertainty. While effective in the short term, they are not seen as sustainable operating models. The implication is a need to formalize decision rights more quickly without institutionalizing chaos.

- Organizations are seeing a shift toward treating disruption as inevitable rather than exceptional. Some acknowledge the challenge of realistically maintaining perfect uptime in extreme scenarios. This reframes cyber response from minimizing disruption to choosing the least damaging form of disruption. As a result, resilience planning is becoming more explicit, deliberate, and business-aligned.

- Another risk is the human capacity and burnout under sustained surge conditions. The anticipated volume of patches, alerts, and response actions introduces a strain that technology alone cannot absorb. While automation and AI can assist, they also introduce new failure modes. This creates a delicate balance between augmenting teams and overwhelming them.

> **“There’s only so much capacity, and the human element of surge is real — burnout is going to be a factor for everyone in this industry.”**
>
> **— Denis Villeneuve, Cyber Resilience and Connectivity Practice Leader, Kyndryl Canada**

Resilience, Containment, and the Shift Beyond Patching

- Identifying crown jewels, critical business processes, and minimum viable operations are foundational to making fast decisions. Without this clarity, organizations risk either overreacting or hesitating at critical moments. This forces tighter integration between cybersecurity, business continuity, and enterprise risk disciplines.

- While defense-in-depth remains essential, reliance on common platforms and providers introduces correlated failure risk. No single control should be assumed infallible. As a result, resilience planning increasingly accounts for control failure as a design assumption rather than an exception.

- The challenges associated with third-party and open-source exposure are renewed in this era. Limited leverage over suppliers, opaque dependency chains, and incomplete software inventories complicate response efforts. This introduces a structural asymmetry where risk materializes faster than visibility. Organizations are therefore re-evaluating how much unmanaged dependency they can tolerate.

"One of the first questions I got from our board was, 'Is this hype or is it real?' From the conversations I've had — it's real."

— Cory Musselman,
Global CISO, Kyndryl

Redefining security for the agentic AI era

Learn more

Leadership, Governance, and Board-Level Reality

- There is a growing recognition that board engagement must evolve alongside the threat landscape. Rather than presenting fixed solutions, leaders are increasingly framing AI-era cyber risk as a discovery and learning journey. This approach prioritizes transparency over certainty, which has been noted as uncomfortable but ultimately more credible.

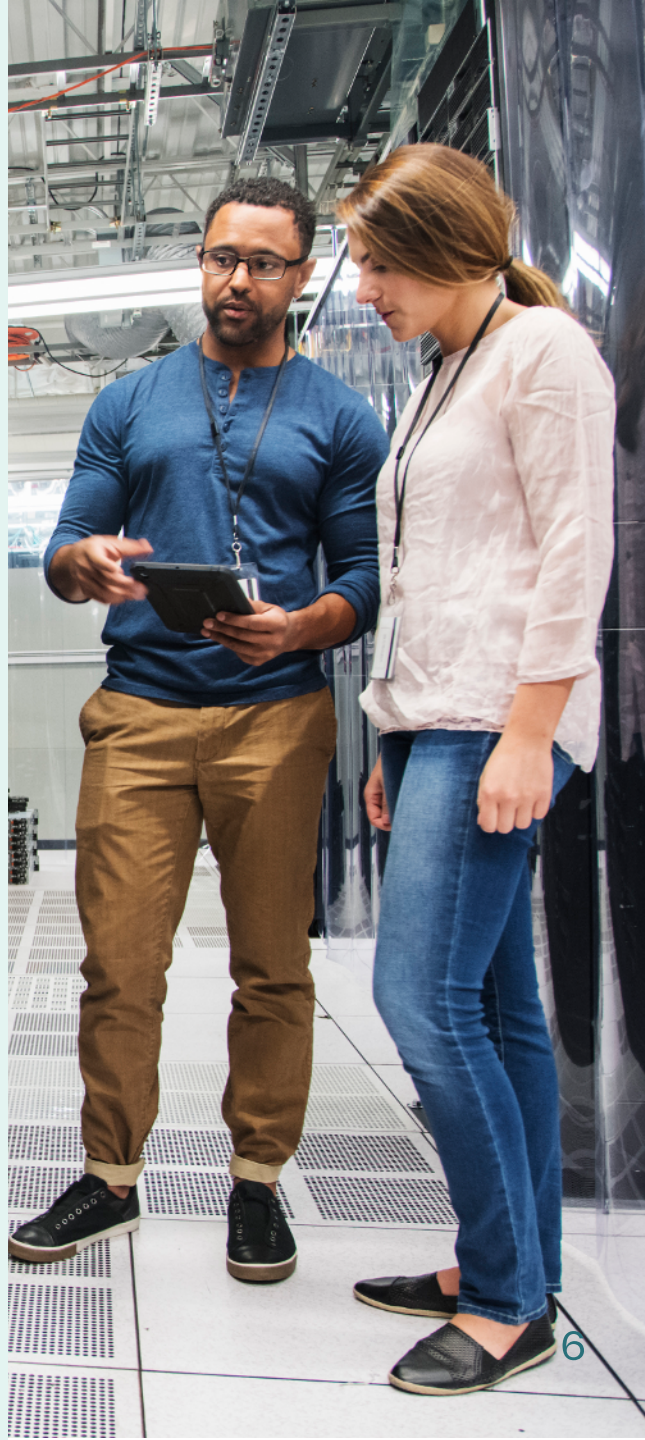
- The governance cadence is changing under accelerated threat conditions. Annual or even quarterly risk assessments were viewed as insufficiently responsive. Organizations are exploring more frequent reassessments to reflect the pace of change. This shift introduces additional governance overhead but is seen as necessary to avoid blind spots.

- Acting too aggressively risks unnecessary disruption, while moving too slowly risks catastrophic exposure. Leaders are therefore being forced into nuanced tradeoff decisions with incomplete information. This reality is reshaping how accountability and decision authority are distributed.

- Executives are increasingly confronting the reality that no organization will solve this challenge alone. Peer collaboration, shared learning, and ecosystem-level coordination are essential to long-term resiliency.

"This is becoming a board-level conversation because remediation speed is no longer a technical metric — it's an operational risk reporting capability."

— Denis Villeneuve, Cyber Resilience and Connectivity Practice Leader, Kyndryl Canada



kyndryl

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