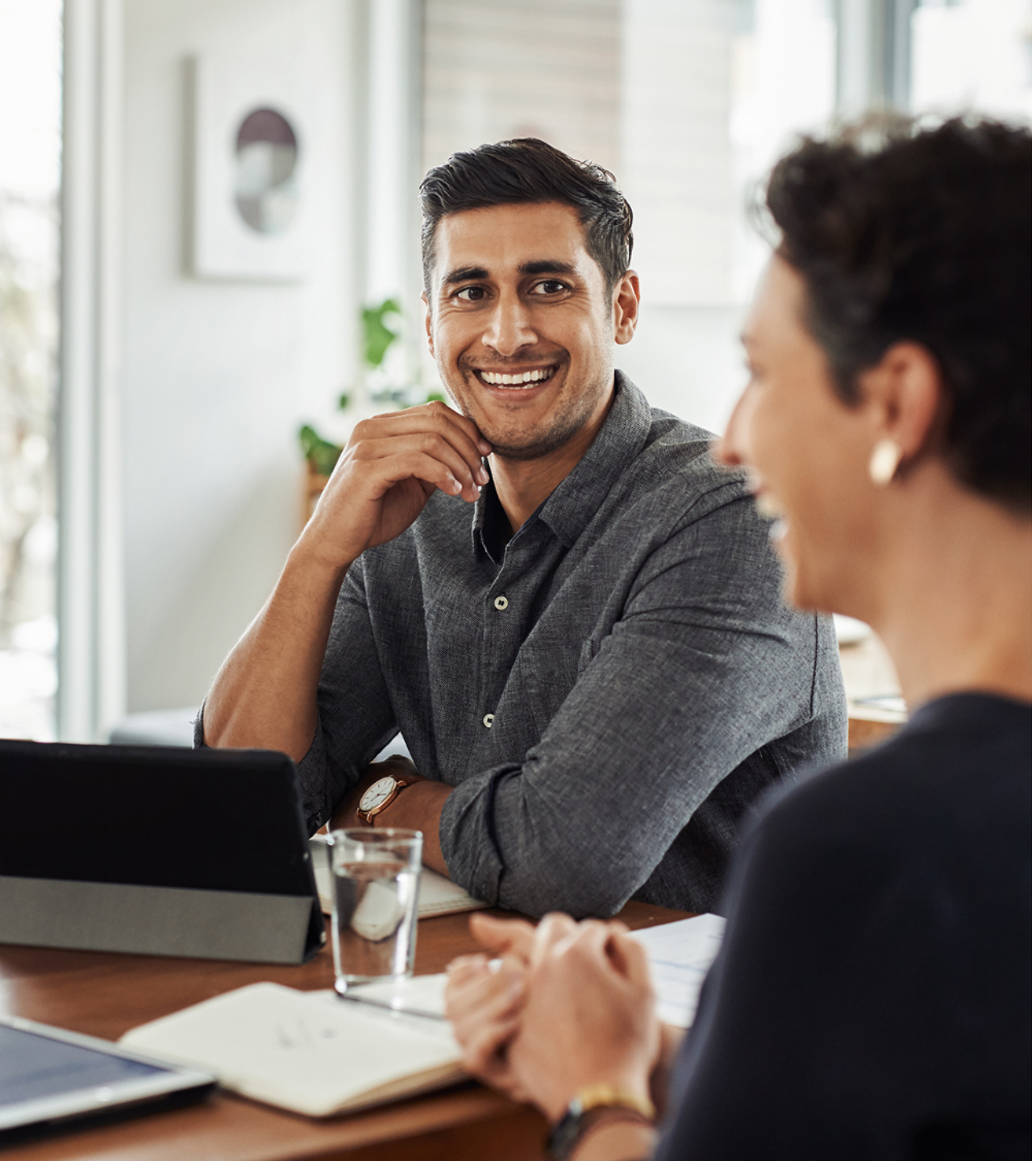
Canada CISO

Expert Exchange

Q2 Executive summary
May 21, 2026

kyndryl



Overview

Senior cybersecurity and technology leaders met to discuss how frontier AI is accelerating vulnerability discovery, compressing remediation timelines, and putting pressure on traditional cyber operating models.

The conversation focused on prioritizing critical vulnerabilities, validating compensating controls, managing third-party and SaaS exposure, and balancing security urgency with business resilience.

Host

Denis Villeneuve
Kyndryl, Canada Cyber Resilience and Connectivity Practice Leader

SME

Cory Musselman
Kyndryl, Global Chief Information Security Officer

Key topics

Compressing Vulnerability Remediation Timelines

- Participants agreed that traditional patching and maintenance windows are becoming increasingly difficult to defend for critical and actively exploitable vulnerabilities. Several organizations are now evaluating or targeting 24- to 48-hour action windows for the highest-risk scenarios, particularly where exposure, exploitability, and business criticality intersect.

- To support faster response, organizations are broadening access to vulnerability data. Rather than relying on security teams as the central bottleneck, application, infrastructure, and frontline operations teams are being given more direct visibility into dashboards, asset context, and remediation queues. This reflects a shift from centralized vulnerability management to distributed operational ownership.

- Participants noted that prioritization must move beyond severity scores alone. Leaders described recalibrating risk models to account for asset criticality, external exposure, data sensitivity, privilege impact, exploitability, time to exploit, and the presence or absence of compensating controls. Identity systems, internet-facing assets, and operational control planes were consistently viewed as requiring the highest level of attention.

- The group discussed whether some patches should be applied more automatically, with remediation resources shifted toward fixing issues after deployment. While this approach may reduce exposure windows, participants also noted that “patch now, fix later” is not appropriate for every environment, particularly where application instability, manufacturing disruption, or core business-service outages could create material operational impact.

"We previously operated on a model where critical system updates needed to occur within two weeks, but that timeline is simply no longer fast enough."

— CISO Expert Exchange Member

Validating Compensating Controls Through Continuous Testing

- When immediate patching is not possible, participants emphasized the importance of compensating controls that reduce exposure and limit blast radius. These include segmentation, isolation, hardening, phishing-resistant authentication, privileged-access controls, external attack-surface reduction, and tighter control of internet-facing services.

- Participants also discussed more precise application-level controls, including allow-listing and schema-based restrictions that limit expected methods, parameters, content types, and data structures. These controls can reduce the opportunity for attackers to explore behavior outside known application boundaries while teams work through remediation.

- A recurring lesson was that compensating controls must be validated, not assumed. Several leaders described the value of automated testing, continuous penetration testing, and internal red-team style validation to determine whether defensive layers actually work in complex environments.

- Participants noted that defenders can gain an advantage by using automated testing tools internally, enriched with knowledge of their own assets, vulnerabilities, network architecture, and business context. This allows teams to identify missing secondary controls, validate attack paths, and prioritize remediation based on real exposure rather than theoretical risk.

- The group also discussed emerging uses of AI to support defensive action, such as generating detection logic or virtual-patching signatures. Participants saw promise in these approaches but cautioned that false positives, noisy outputs, and operational impact still require human review and careful tuning.

"Focus heavily on maintaining your mitigating controls and limiting the blast radius, because those protective layers will buy you valuable time."

— CISO Expert Exchange Member

Managing Third-Party, SaaS, and Supply Chain Exposure

- Participants highlighted that third-party and SaaS risk is becoming more direct and urgent as remediation timelines compress. Many organizations depend on critical vendors for essential business processes but have limited visibility into whether those suppliers can patch, virtually patch, or otherwise mitigate vulnerabilities at the pace now expected.

- Leaders discussed moving beyond generic compliance questionnaires toward more targeted supplier engagement. One emerging approach is to first define minimum viable operations and identify the suppliers that support those essential services. This allows organizations to prioritize direct cybersecurity discussions with the vendors that matter most to operational continuity.

- Participants noted that contractual and practical leverage over critical suppliers can be limited, particularly when vendor patching timelines do not align with internal remediation expectations. This is prompting organizations to reassess supplier expectations around transparency, incident escalation, evidence of remediation, and response timelines.

- External risk-rating and monitoring platforms were discussed as one way to infer supplier security posture from observable internet-facing signals. Participants acknowledged that these tools can provide useful evidence for vendor conversations, but also noted that they may not reveal internal application risk, operational dependencies, or unexposed vulnerabilities.

- The group also discussed the likelihood of subsequent supply-chain waves. Larger technology providers may be better positioned to absorb the cost and operational burden of AI-enabled vulnerability discovery, while smaller software, SaaS, and open-source providers may face greater pressure if they lack access to comparable tooling or remediation capacity.

"We have critical business processes dependent on key vendors, but we often have no way to confirm they are securing their environments in a reasonable fashion."

— CISO Expert Exchange Member

Balancing Remediation Speed with Business Resilience

- Participants emphasized that accelerated remediation must be balanced against business continuity, user experience, and operational stability. Frequent reboots, short restart windows, and fragmented patch deployment can disrupt meetings, reduce productivity, and create pushback if not managed carefully.

- Organizations are experimenting with different enforcement models, including time-zone-aware patching, end-of-day reminders, limited postponement options, countdown warnings, and more aggressive restart policies for the most critical issues. The appropriate model depends on business context, endpoint type, exposure, and the effectiveness of surrounding controls.

- The group noted that some environments cannot absorb disruption in the same way as standard corporate endpoints. In manufacturing, OT, critical infrastructure, or other continuous operations environments, uncoordinated maintenance can create revenue loss, safety risk, or service disruption. Participants agreed that security action must be risk-based and aligned to business impact, not blindly enforced.

- Participants also discussed scenarios where patches may not be available quickly, including end-of-life systems, open-source dependencies, and operational technology environments. In these cases, isolation, monitoring, hardening, virtual patching, and recovery planning become essential parts of the response strategy.

- Leaders reinforced that resilience planning must move beyond executive tabletop exercises. Organizations need technical and operational drills that test runbooks, recovery sequencing, failover assumptions, escalation paths, and cross-functional decision-making under pressure.

- Participants also stressed the importance of filtering vendor hype from practical action. Rather than responding to fear-based messaging, organizations are focusing on fundamentals: asset visibility, exposure management, control validation, incident readiness, and the ability to continue operating through disruption.

"If you start to disrupt the business too much, no matter how important of a cyber issue it is, you are not functioning as a business anymore."

— CISO Expert Exchange Member

kyndryl

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