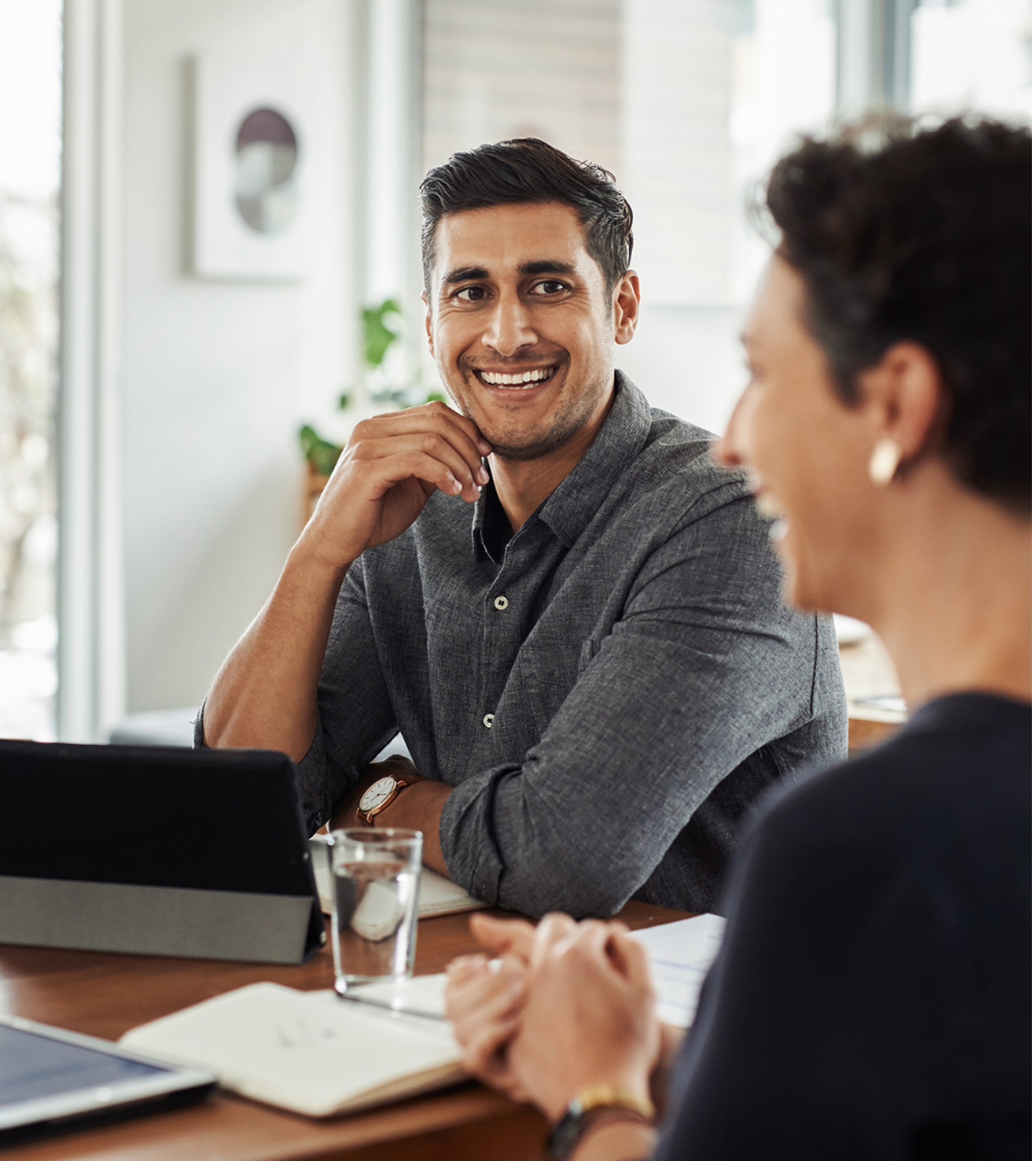
Canada CISO

Expert Exchange

Q1 Executive summary
March 5, 2026

kyndryl



Overview

A recent roundtable discussion brought together senior cybersecurity leaders to exchange strategies for organizational defense and system reliability. Members discussed rethinking business recovery strategies, validating the security of external service providers, automating identity and access governance, managing the unique risks introduced by autonomous artificial intelligence programs, and balancing internal software testing methodologies.

Host(s)

Denis Villeneuve
Cybersecurity and Resilience Practice Leader, Kyndryl Canada

Shawn McGuire
Practice Partner, Security and Resiliency, Kyndryl Canada

Jackie Flowers
Global IAM Domain Lead
Kyndryl

Key topics

Rethinking Business Resilience and Operational Recovery

- Executives must transition from preparing for massive site failures to continuously testing the reliability of individual business components and third-party services.

- One security leader argued that the traditional approach of preparing for complete facility losses no longer satisfies modern auditing requirements, which now demand greater precision. Instead, organizations must narrow their focus to thoroughly understand how isolated events, such as losing login access to critical providers for twelve hours, directly impact overall corporate operations and workforce productivity.

- Participants generally agreed that defining a minimum viable company helps organizations isolate the exact critical processes required to maintain fundamental operations during a crisis. By breaking complex environments into smaller, manageable segments, security teams can conduct targeted technical exercises much more frequently and build greater confidence in their localized recovery strategies.

- Another participant noted a significant disconnect between business partners and technical realities, as non-technical executives often assume security systems remain available indefinitely. Clearly communicating the actual recovery limitations of these platforms has revealed new investment opportunities, prompting the creation of secondary emergency access methods to ensure executives can connect during widespread outages.

"Resilience cannot remain an annual testing event; it must become an everyday operational reality where teams regularly evaluate critical business connections."

— CISO Expert Exchange Member

The CEO tipping point: reckoning with the new reality

Learn more

Validating External Service Provider Security

- Organizations struggle to accurately measure the security of external service providers, relying on a mix of independent compliance certifications and direct system testing, but feeling that there is room for improvement.

- A debate emerged regarding the true value of independent compliance certifications provided by external software vendors. One participant expressed deep skepticism about relying on these standard reports, warning the group that trusting them alone creates a false sense of security about the actual financial and operational risks external providers introduce to the business

- Leaders shared diverging views on their practical ability to independently test external platforms for dangerous vulnerabilities. One executive highlighted their past success using independent reward programs and ethical hackers to force external vendors to fix security gaps. Others from smaller organizations argued they completely lack the negotiating leverage required to demand such aggressive testing rights.

- There was interest in using AI to create engaging and informative security training videos, providing a scalable solution to educate employees on security practices. The AI video-generator tool mentioned during the conversation was Synthesia.

> **"How much influence do we as consumers of cloud applications truly have over the defensive posture of our service providers?"**
>
> **— CISO Expert Exchange Member**

Automating Identity Governance and Access Reviews

- Companies are aggressively upgrading their user access governance from manual spreadsheets to automated systems that enforce strict controls and immediately remove inactive accounts.

- One executive shared a highly successful transition from a manual spreadsheet review system that suffered from low participation to a modern, fully automated platform. This strategic shift immediately achieved full management participation across the company and exposed hundreds of excessive user permissions, which the security team quickly revoked, drastically reducing the organization's overall vulnerability footprint.

- While attendees strongly agreed on the value of automation, one participant warned against treating access reviews merely as a routine compliance exercise designed solely for auditors. They argued that executives must prioritize building a strong foundational process that ensures the immediate, automated removal of access the moment an employee changes roles or departs the company.

- To combat the dangerous buildup of excessive permissions when staff members switch departments, experts recommended linking identity platforms directly into sensitive administrative environments. Tracking the last active login date provides irrefutable evidence for removing human access, though attendees conceded this measurement proves difficult to apply to automated system accounts that lack traditional login behaviors.

"If managers assign and remove user permissions correctly in the first place, auditors would find absolutely nothing left to review."

— CISO Expert Exchange Member

Governing Autonomous Artificial Intelligence Programs

- The rapid corporate adoption of autonomous artificial intelligence systems introduces an urgent governance challenge, as current tools fail to monitor programs that independently alter their own behaviors.

- One member raised a concern about the aggressive deployment of artificial intelligence systems across their enterprise environment. They highlighted a severe lack of commercial tools capable of effectively managing the scope of access for autonomous programs that communicate directly with other systems, operate without human oversight, and execute tasks using shared company data.

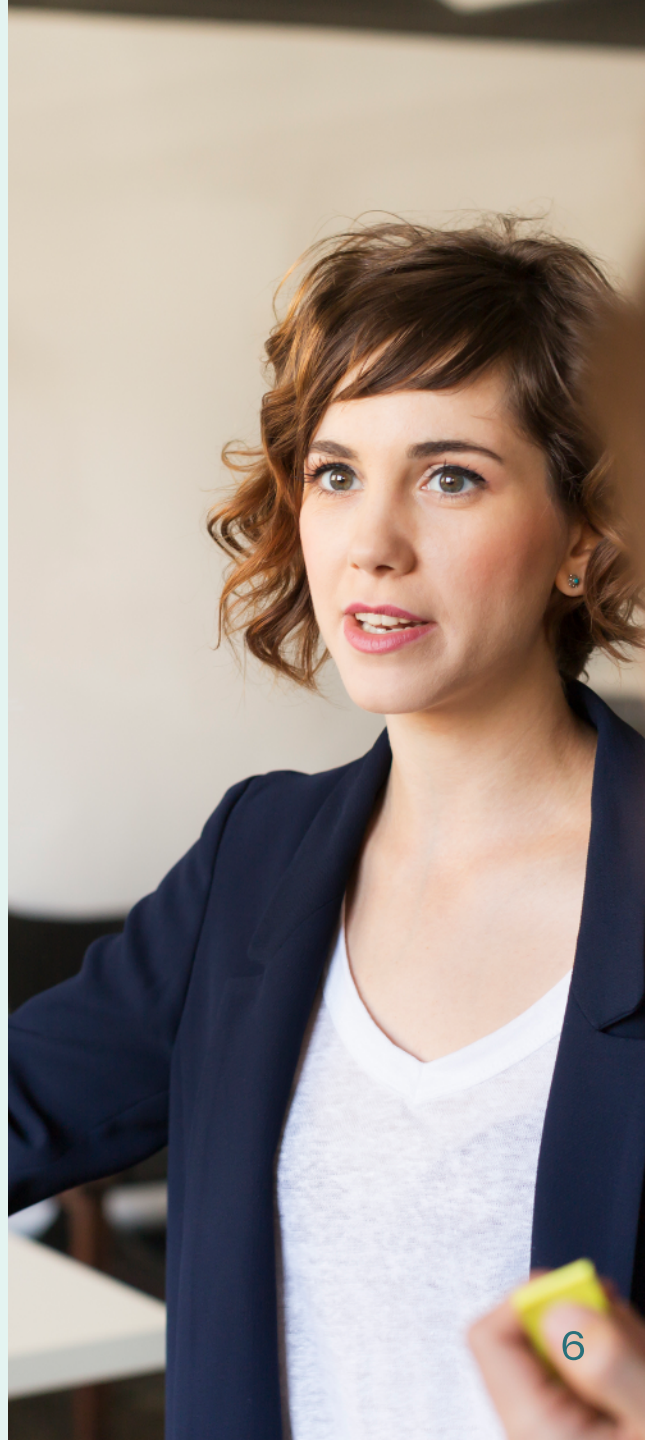
- The group discussed how to accurately assess the long-term risk of these emerging technologies before granting them network access.

  One leader suggested that governance teams could successfully rely on a thorough initial risk assessment to fully understand the program's intended function, assigning a strict expiration date to its access to prevent unchecked future activities.

- However, others disagreed with this simplified approach, arguing that artificial intelligence systems remain uniquely complex, specifically because they adapt continuously based on new inputs. An automated program initially authorized for a specific task might, over time, change its function independently, leaving security teams completely blind to its evolving actions and newly acquired data permissions.

"When autonomous programs utilize their own feedback loops to learn and communicate, whose context actually carries through the chain of communication?"

— CISO Expert Exchange Member



Balancing Internal Software Testing Methodologies

- Organizations balance different internal software testing strategies, debating whether to provide full system access to testers or require them to operate blindly to simulate real-world attacks.

- Participants shared diverse strategies for testing the security of their internal applications and explored the benefits of providing testers with complete system knowledge. One member noted they provide their testing teams with full architectural documents and source code, prioritizing the discovery of all possible vulnerabilities over simulating a blind external attack.

- Conversely, other attendees argued for alternative approaches, noting they start their testing teams with zero system knowledge to observe how external threats might navigate the environment. However, they agreed that if testers encounter significant roadblocks, granting them partial access would ensure the exercise continues to produce valuable insights within the designated timeframe.

- The conversation also highlighted the growing importance of securing application programming interfaces, which connect different software systems behind the scenes. Security leaders agreed that these interfaces require the exact same rigorous testing applied to traditional consumer-facing applications, as they represent hidden pathways that malicious actors frequently target.

> "We supply our internal testing teams with comprehensive system architecture documents so they can expose every possible vulnerability before we launch."
>
> — 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.