

Rapid Remediation and Governance Beyond Patching

Insights from the Kyndryl Security & Resilience Expert Exchange on July 14, 2026

kyndryl®



Contents

01

Reimagining
remediation and
resilience

02

Remediation and
resilience must move
faster, together

03

Boards are engaged,
but their crisis role
must be bounded

04

Patching alone cannot
solve machine-speed
risk

05

AI-assisted dev: better
engineering
governance exposure

06

Suggestions for
defending at machine
speed

07

What is the Kyndryl
CISO Expert Exchange?

08

Kyndryl cyber
resilience services

01

Reimagining remediation and resilience

Security leaders are confronting a threat environment that is moving faster than traditional vulnerability-management programs were designed to handle.

The rise of frontier and agentic AI has intensified pressure to shorten remediation windows, automate more of the patching lifecycle, and make boards more comfortable with the operational disruption that follows.

In this context, CISOs are working through some targeted challenges:

- Accelerating remediation without making resilience an afterthought
- Involving boards in crisis planning
- Employing strategies like isolation and deception where patching cannot keep pace
- Building the governance and engineering capability needed for AI-assisted development

Kyndryl hosted a CISO Expert Exchange to explore these issues and best practices for approaching them.



02

Remediation and resilience must move faster, together

Security teams are compressing critical patch timelines as AI-enabled attackers shrink the distance between vulnerability discovery and exploitation. Some organizations still operate on monthly cycles for routine patching, while others are pushing five-day windows for critical, high and known-exploited vulnerabilities. Several organizations have taken that expectation directly to the board.

Security leaders are framing rapid remediation as an enterprise risk decision, not just a technical one. Faster fixes can disrupt tools and processes, requiring strong rollback discipline. Organizations are revisiting business continuity plans, testing manual operations during outages, and defining minimum capabilities needed to sustain operations. For environments with technical debt or complex application portfolios, success extends beyond patch speed to building resilience—the ability to absorb disruption and maintain essential services.

Multiple participants stated that both their executives and boards are now expecting them to break things on a regular basis as a result of Frontier AI. comfortable with the operational disruption that follows.

How Frontier AI is
reshaping risk



03

Boards are engaged, but their crisis role must be bounded

AI-enabled threats are generating board interest that security leaders have struggled to generate through ordinary tabletop exercises. Several participants described boards asking to participate more directly in business-continuity and incident-response simulations. CISOs welcomed this development because engaging boards in this way can increase their support for funding, sharpen executive attention and expose governance gaps before a real emergency.

However, this opportunity comes with a practical challenge: Board members often enter simulations with the instinct to direct the response rather than observe, ask oversight questions and let management execute the plan. Participants emphasized that tabletop exercises should be used to set those expectations before a crisis.

In one example described by a participant, board members performed well during a real incident when they were informed and allowed the operational response to proceed but struggled during a later tabletop because the structure invited more direct decision-making. The lesson for CISOs is to design board participation intentionally, make the oversight-versus-operations boundary explicit and treat the exercise as a rehearsal for governance behavior as much as a test of the technical response plan.



Participants emphasized that boards are not supposed to be making operational decisions in a tabletop exercise, but that they have a difficult time not expressing an opinion on the right direction and course of action.

04

Patching alone cannot solve machine-speed risk

Participants were clear that faster patching is necessary but insufficient, especially in operational technology, healthcare delivery, manufacturing, distribution, higher education and heavily customized enterprise environments. Off-lying a plant, robotics-enabled distribution center or clinical system can create more business risk than the vulnerability itself.

As a result, organizations are being selective about where selective automation is appropriate. The conversation is moving from vulnerability management alone toward continuous threat exposure management, where patching is one control among many rather than the entire strategy.

Reducing blast radius is becoming as important as reducing vulnerabilities, with several participants highlighting segmentation as a critical.

“You can’t out-patch AI. The challenge is balancing rapid remediation with operational resilience..”

CISO Expert Exchange participant



05

AI-assisted development requires better engineering and governance

The same AI tools that can strengthen vulnerability detection are also expanding the attack surface. Participants described developers and business users pulling in elements and components they do not fully understand, while AI-generated coding behavior can trigger security alerts because it resembles non-human attacker activity. Open-source components, vendor-managed libraries, and hidden dependencies are already difficult to inventory, and AI-assisted coding increases the volume and speed at which those dependencies can enter the environment.

In response, security teams are investing in application-security culture, AI-enabled code-review tooling, static and dynamic scanning, open-source dependency checks, and governance workflows that examine which data sources new AI tools access before they move toward production.

More broadly, security leaders are trying to shift their teams from a buy-first model to one with stronger engineering capability. They are automating administrative work, consolidating platforms, building internal review processes, and developing the skills to test and tune AI capabilities rather than simply purchase another tool. The budget conversation is becoming as much about skill transformation and operating model maturity as it is about tooling.



06

Suggestions for defending at machine speed

The following suggestions for this dynamic era in security operations emerged from the discussion:

- Communicate to executives that faster remediation comes at a cost: broken tools, disrupted processes and the need for rapid rollback discipline.
- Make explicit to boards that their role in tabletop simulations is to observe and learn, so that these exercises are as much governance rehearsals as they are technical tests.
- Move from patching alone to employing layered controls that buy time, obscure fragile assets, and make attacker movement easier to detect.
- Shift security teams toward a focus on working to engineer proprietary, custom solutions instead of buying third-party tools for every challenge.

→
Reallocating cybersecurity capital in the Mythos era



07

What is the Kyndryl CISO Expert Exchange?

The **Kyndryl CISO Expert Exchange** is a curated, peer-driven program that brings together CISOs and senior IT leaders for meaningful collaboration and shared learning. There are CISO Expert Exchange communities in the U.S., Canada and Europe.

The July 2026 conversation was moderated by **Adeel Saeed**, SVP, Technology Strategy and Execution Management CTO, Global Cyber Resiliency at Kyndryl.



Adeel Saeed

*SVP, Technology Strategy and Execution Management
CTO, Global Cyber Resiliency*

[Visit Kyndryl CISO Expert Exchange](#)



08

Kyndryl cyber resilience services

Kyndryl helps organizations transition from their current infrastructure to a high-performance, AI-native future. Our security and resiliency services are designed to accelerate growth and innovation, offering scalable solutions that protect data and AI assets, ensure compliance, and stay ahead of emerging threats. We secure mission-critical infrastructures and develop AI-native capabilities by combining strategic advice with hands-on execution, empowering leaders to confidently pursue growth and innovation. Learn more at [Kyndryl.com](https://kyndryl.com).





© Copyright Kyndryl Inc. 2026. All rights reserved.

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.