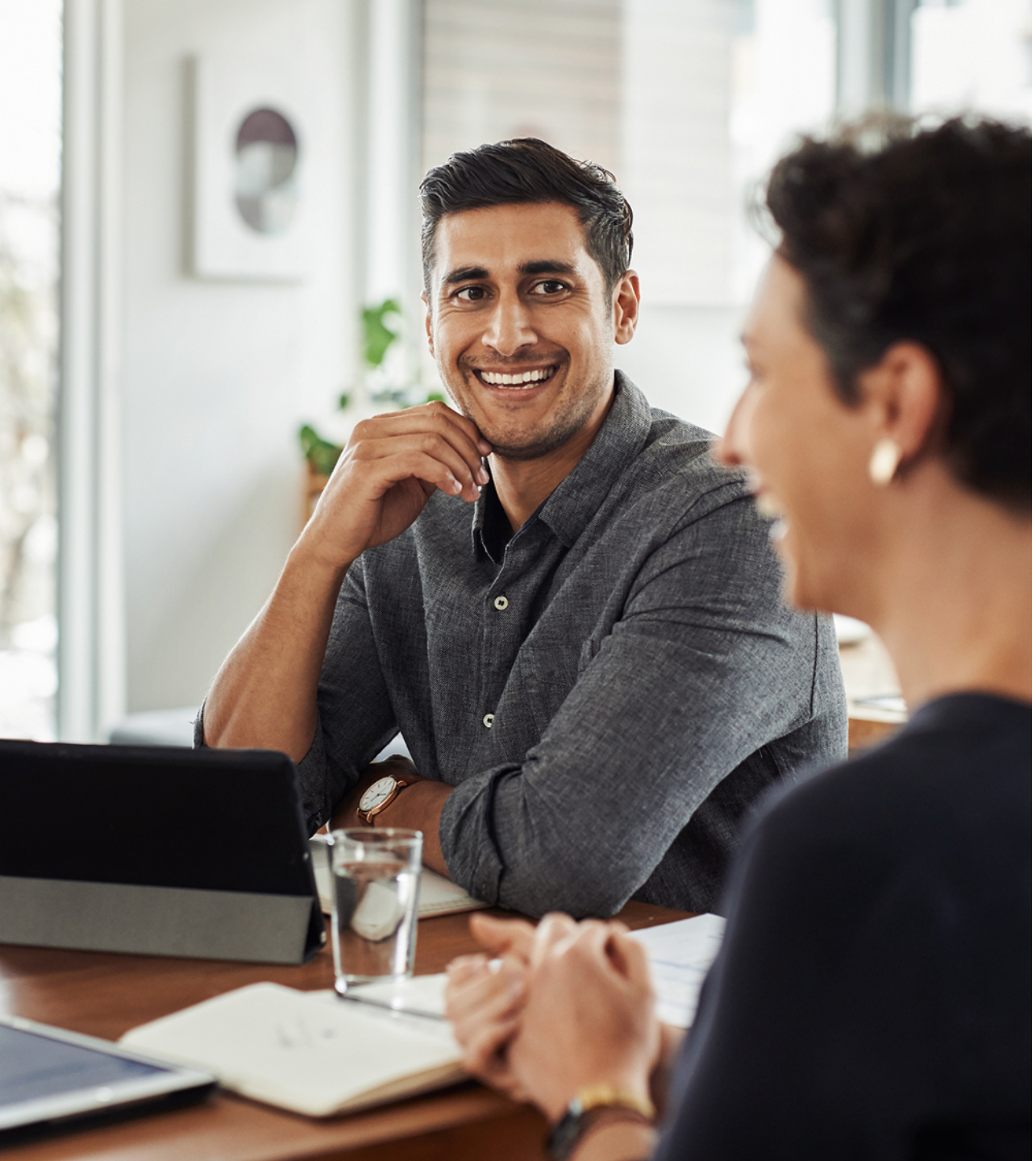
Executive Summary

# Security and Resiliency Expert Exchange

November 18, 2025

kyndryl



# Overview

A group of global security and resilience experts convened to discuss recent cybersecurity incidents, using the F5 breach as a case study to highlight key priorities for business executives: phased incident response, stronger supply chain governance, architectural resilience, and robust third-party risk management.

These measures help reduce exposure and maintain trust in a complex threat landscape.

# Host & SMEs

**Conal Hickey**
Vice President
Security and Resiliency, Kyndryl

**Jimmy Nilsson**
Vice President of Professional Zero (Zero Trust), Kyndryl

**Anthonie De Bos**
Vice President
Security and Resiliency, Kyndryl

# Key topics

# Strategic Response to a Major Vendor Compromise

- The incident, where the attacker accessed and stole the vendor's proprietary source code, created a high-risk scenario that requires a structured, multi-phased approach to risk mitigation. The theft of source code increases the likelihood of future, difficult-to-detect attacks because malicious actors can analyze the code to uncover hidden vulnerabilities and exploit them over time.

- Organizations should adopt a three-phase response plan when a critical vendor experiences a source code compromise: immediately apply patches and necessary hardware upgrades, implement compensating controls to minimize risk from unknown future vulnerabilities, and finally, evaluate alternative technology solutions if needed.

- CISOs emphasized that implementing compensating controls is critical. Key measures include enforcing multi-factor authentication for management interfaces, restricting access to specialized and secure infrastructure, and applying privileged access management to safeguard administrative credentials.

- Experts noted diverging views on acceptable risk after the incident. One large organization with air-gapped protection felt the risk remained too high and decided to migrate off the technology, while a major bank, using the system only for basic traffic balancing, considered patching unnecessary. This illustrates that risk tolerance is highly situational and depends on the role the technology plays within the business.

- To prepare for unknown vulnerabilities, organizations should implement micro-segmentation for compromised systems. This limits unauthorized lateral movement within the environment if a vulnerability is exploited. The conversation also encouraged moving from standard encrypted communication protocols to mutual encryption between devices and downstream systems to strengthen authentication and security.

"Tactical response involves patching as a crucial first step; this is the process we followed and advised clients to implement, followed by compensating controls, and evaluation of alternatives."

— CISO Expert Exchange Member

**When the foundation is breached: Lessons from the F5 incident**

**Learn more**

# Securing the software supply chain and source code integrity

- The recent compromise prompted detailed discussions on internal source code security, particularly the risk of relying on external services for vulnerability scanning. Executives must weigh the security benefits of using external tools against the inherent risk of exposing sensitive assets, ensuring decisions align with both risk tolerance and compliance requirements.

- Experts debated the trade-off of adopting cloud-based source code scanning solutions: while these services enhance security by identifying flaws, they require transferring the organization's proprietary source code to a third-party cloud environment, introducing a new threat vector.

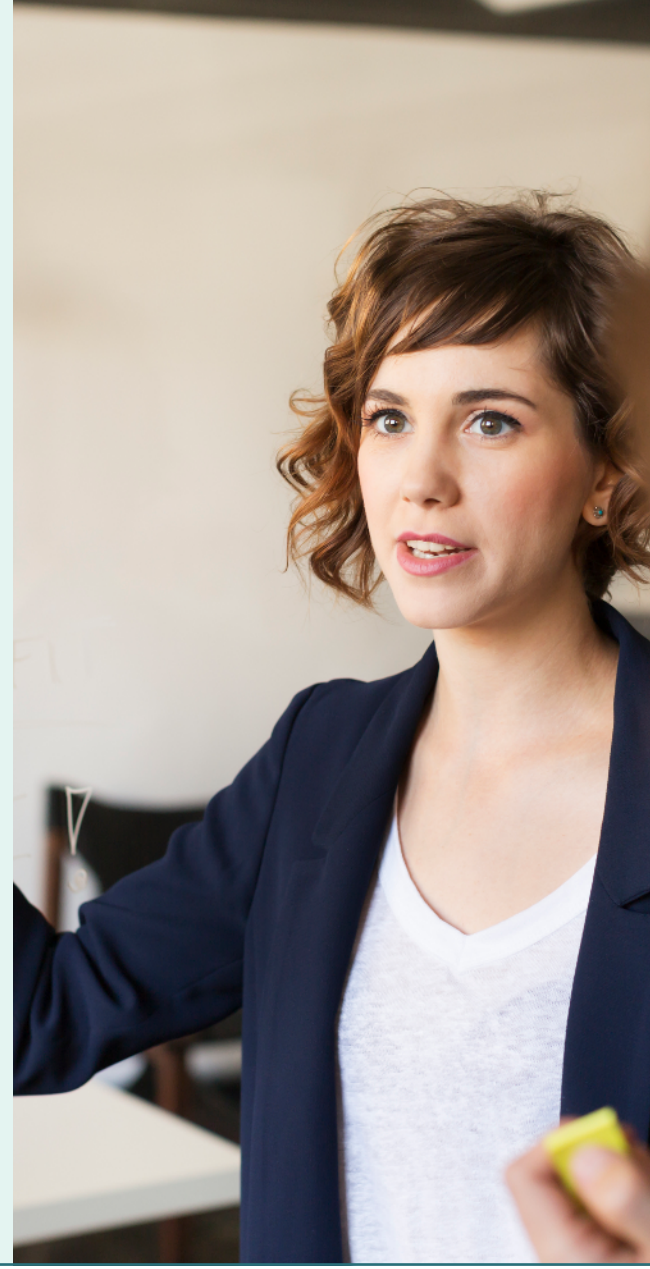
- A key learning shared by participants was that the criticality of the source code should drive the decision. Organizations must assess the potential impact and damage of disclosure before making a risk-based decision about using external services.

- A global risk leader stressed the importance of robust source code management, urging organizations to maintain full visibility and control over all components and modules within their codebases, as attackers often exploit changes or swapped modules.

- One executive shared that their organization is shifting security responsibility left — integrating automated code checks into the development pipeline and blocking progress if vulnerability thresholds are not met. This cultural shift is reinforced by improving developer security iteracy through ongoing training and events, recognizing that centralized security teams cannot manage all risks alone.

- There was a counterargument that transparency is critical, with one expert suggesting that organizations should require a Software Bill of Materials List from vendors to better understand the code they deploy, moving beyond basic contract-based risk assessments.

> **"We are struggling with a dilemma: while using a cloud-based application security tool helps identify vulnerabilities, it also increases the risk of source code disclosure, similar to the recent vendor breach."**
>
> **— CISO Expert Exchange Member**



# Building Cyber Resiliency through Zero-Trust Architecture

- Given that organizations cannot avoid all breaches, the focus must shift toward building inherent resilience into the security architecture to limit damage and accelerate recovery. Zero Trust provides the methodology needed to achieve this resilience.

- Zero Trust is defined as a methodology or strategy, not merely the adoption of a new security technology. It guides organizations in creating greater resiliency within core systems.

- The approach begins with a comprehensive understanding of all critical assets that require protection, followed by integrating existing security capabilities so they share intelligence and make smarter enforcement decisions. This integrated approach ensures that various security controls reinforce each other.

- Participants agreed that resiliency is the fourth phase of this strategic methodology, following asset identification, integrated controls, and improved detection. This phase focuses on establishing recovery capabilities in the event of an unexpected breach.

- Experts advised that true cyber resilience depends on executives knowing their critical business processes end-to-end, not just in a traditional disaster recovery sense. This means understanding the application and infrastructure flows supporting core business functions and deploying technical controls like isolated, immutable storage vaults for rapid data restoration.

- The functional role of the Security Operations Center (SOC) is expanding beyond merely detecting incidents to anticipating threats and actively managing recovery. This transition transforms the SOC into a "security risk center" that supports the proactive recovery or rerouting of services in collaboration with network teams.

"It is nearly impossible to prevent all impacts from sophisticated attacks; therefore, organizations must focus on architecting robust security measures to become significantly more resilient."

— CISO Expert Exchange Member

The Kyndry Zero Trust framework

**Learn more**

# Balancing Risk in Third-Party Management and Visibility

- Executives must address the difficult balance between regulatory requirements demanding deep supply chain visibility and the practical inability of most organizations to conduct comprehensive audits of every vendor.

- CISOs questioned how many tiers of the supply chain organizations should examine, noting that heavy reliance on standardized security scores often reduces meaningful, qualitative insight into a supplier's actual security practices.

- One executive strongly argued that global regulation requiring audits of major suppliers are unrealistic for small or medium-sized businesses, drawing an analogy to a customer being forced to check the security supply chain of every car component within the new car they purchase. This viewpoint suggests that prioritizing internal detection and resilience remains the most practical approach.

- Regardless of size, participants agreed that when organizations onboard a critical third-party service, that supplier effectively becomes an integrated security partner. Organizations must avoid treating them as an "unattended supplier" by implementing controls, monitoring, and audit processes to ensure security measures are maintained.

- The conversation highlighted that regulatory pressure is mounting (for example, specific EU mandates require companies to contractually retain the right to audit suppliers), often without regard for the auditing capabilities of the regulated entity. Because of this, some organizations are leveraging their technology partners to conduct necessary service checks and pre-vetting across their shared customer base.

"The expectation that small companies should conduct in-depth security audits of major global technology suppliers is unrealistic, highlighting a disconnect between regulatory requirements and practical capability."

— CISO Expert Exchange Member

**Continuous Control Monitoring: A proactive approach for a more resilient future**

**Learn more**

kyndryl

The Security and Resiliency Expert Exchange is hosted by Kyndryl. Please contact Conal Hickey with any questions about Kyndryl or this Exchange.