CIONET

DISCUSSION SUMMARY

MANAGING COMPLEXITY, RESILIENCE AND TRUST ACROSS A NATIONAL RAIL TECHNOLOGY ESTATE

The session explored the technological, organisational and cultural challenges of running one of the UK's most complex operational infrastructures: the national rail IT and telecommunications estate. The discussion centred on leadership during disruption, the role of partners across a vast supply chain, and the increasing pressures of cyber resilience in a highly regulated environment.

The CIO's reflections provide a candid view into the realities facing critical national infrastructure (CNI) leaders: ageing systems, organisational fragmentation, heightened public scrutiny, and a rapidly evolving threat landscape that requires both defensive strength and fast, disciplined recovery.

1. The CIO Role in a Shifting Rail Landscape

Over recent years, the CIO remit has expanded significantly. Beyond the traditional management of corporate IT, the role now spans:

- National data centres hosting systems ranging from 1970s legacy platforms to newly deployed applications.
- Infrastructure supporting c.45,000 Network Rail staff and an additional 15–20,000 supply-chain and partner personnel.
- Management of one of the UK's largest telecoms networks – a hybrid between a BT-style transmission backbone and a Vodafone-type service, including a dedicated 2G network used for operational communications.

The CIO offered these key operational lessons for maintaining operational excellence, which are essential for the management of this critical 2G platform, train-to-control and ship-to-shore communications:

- Rigor in Change Management: Exercising extreme care when undertaking critical changes, recognising that the complexity of legacy systems demands meticulous planning to avoid unintended consequences.
- Configuration Integrity: Maintaining a robust and documented configuration level to prevent drift and ensure the system operates reliably.
- Risk Mitigation and Planning: Ensuring strong back-out plans are in place and regularly tested, alongside a comprehensive understanding of the full impact of any system change before execution.

- Human Resilience and Preparedness: Actively mitigating knowledge fade through the requirement for regular rehearsal in contingency plans among response teams, recognising that operational resilience is ultimately dependent on human capability and preparedness.

With Great British Railways (GBR) on the horizon, the CIO is navigating an unprecedented period of transition. Fourteen train operating companies will gradually move under the GBR umbrella, yet no parent entity exists today to absorb them. This creates a quasi–mergers-and-acquisitions environment without a conventional corporate structure, requiring careful choreography to avoid disrupting the live railway.

2. Partnering at Scale: Building Trust Across a Vast Supply Chain

Roughly 80% of technology spend flows through partners, making supplier relationships fundamental to service stability.
Key points raised:

- The end-to-end delivery chain for even a single service can stretch from a data centre, through multiple network and middleware layers, all the way to end-user devices with multiple suppliers involved at each step.
- During major incidents, finger-pointing can be common. The CIO emphasised the importance of stripping this out: “If the boat is taking on water, we all drown unless we fix the hole.”
- Success relies on treating partners as an extension of the internal team. This includes inducting supplier staff into the culture, explaining the realities and risks of the railway, and recognising positive contributions publicly, where procurement rules allow.

The mobilisation phase matters

Where supplier relationships have worked best is in the mobilisation period following contract award. Time spent early on understanding context, building relationships, and aligning expectations prevents misunderstanding later.

3. Creating Operational Resilience: Discipline Over Heroics

One of the strongest messages was that reliable service is less about “hero” behaviour and more about disciplined execution.
Foundations of resilience:

- Rigorous change management: Clear plans, rehearsed back-out processes, unambiguous communication routes and escalation paths.
- Regular testing: The December outage reinforced how easily knowledge fades when contingency procedures aren’t used often.
- Cultural accountability: Placing service performance on the corporate scorecard keeps resilience a shared responsibility.

Over a five-year period, this disciplined approach has helped raise availability from around 98.5% to consistently above 99%, despite the complex mix of legacy and modern systems.

4. Cyber Security: Accepting That Recovery Is as Important as Defence

Cyber threats remain the CIO’s biggest worry.

Notable themes:

- The sophistication of attacks, often aided by readily accessible AI tools, has accelerated. Capabilities previously exclusive to state-backed actors are now available to curious individuals.
- Following the high-profile Wi-Fi splash-page incident at major stations, the CIO stressed the need for transparency across the entire supply chain, not just direct contractors.
- Recovery is now as critical as prevention. The CIO must challenge all business leaders as to how they run their part of the business without IT, how practiced are you and do you actively practice for crisis execution. This is beyond disaster recovery.
- The forthcoming Cyber Resilience Act will likely increase scrutiny, obligations and cost across suppliers, leading to higher risk premiums in contracts

5. Culture, Behaviour and Safety: A Distinctive Advantage

A recurring message was the importance of embedding suppliers into the rail culture, particularly the safety culture.

Examples include:

- Mandatory adherence to Network Rail's life-saving rules (e.g., no handheld device use while driving).
- Bringing partners on site: into control rooms, depots and operational environments, so they experience first-hand the conditions staff work in and the real-world consequences of system failures.

This cultural alignment strengthens empathy, shared purpose, and ultimately trust across multi-party delivery models.

6. Leadership Reflections and Skills for the Modern CIO

The discussion briefly turned to the evolving CIO profile. Points raised included:

- CIOs increasingly require broad business literacy, not just technical depth.
- The profession still struggles with perceptions of technologists being "too narrow," though this is changing as technology becomes inseparable from organisational strategy.
- Continual learning is essential; the CIO referenced turning dense research papers into audio content for consumption while running, an example of adapting personal learning habits to stay current.

7. Balancing Cyber Spend

A question was raised about whether organisations should invest more heavily in proactive defence or recovery capabilities. The CIO's view was unequivocal:

- Zero trust and strong defence are essential,
- but no organisation can defend against everything.
- It is no longer "if" but "when."
- Budget must be balanced across defence, detection, response and recovery, with recovery treated as a business, not purely technical, process.

Conclusion

The session highlighted the complexity, scale and visibility of running technology within critical national infrastructure. The overarching lessons were:

- Resilience comes from discipline, rehearsal and clarity, not luck.
- Recovery capability is now as vital as prevention.
- Partner ecosystems succeed when culture, understanding and shared purpose are deliberately cultivated.
- As GBR emerges, integration activities will resemble long-running M&A programmes, demanding careful governance to avoid destabilising operations.
- And finally, the CIO of the future must be an interpreter between disciplines, equally comfortable in technology, business and crisis leadership.

CIONET

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.