METIS INTELLIGENCE
Issue 001 · RESEARCH SERIES



From Cybersecurity to Operational Resilience

What European Railway Leaders Told Us About Managing Cyber Risk in an Increasingly Connected Railway

July 2026

What determines whether a railway can continue operating when cyber incidents occur?

This report explores what experienced practitioners consistently told us.

Contents

PART ONE

Understanding the Shift

Executive Summary 04

How This Research Was Conducted 06

Editorial Principles 08

The Current State 10

PART TWO

Research Findings

From Cybersecurity to Operational Resilience 14

Governance Across Boundaries 18

Mapping Interdependencies 22

The Visibility Gap 26

Culture and Human Factors 30

PART THREE

Synthesis and Outlook

Cross-Cutting Themes 34

Five Strategic Shifts 38

Research Confidence Matrix 42

Looking Ahead 44

Research Integrity Statement 46

Executive Summary

> Our research indicates that European railway organisations are changing the way they think about cyber resilience.

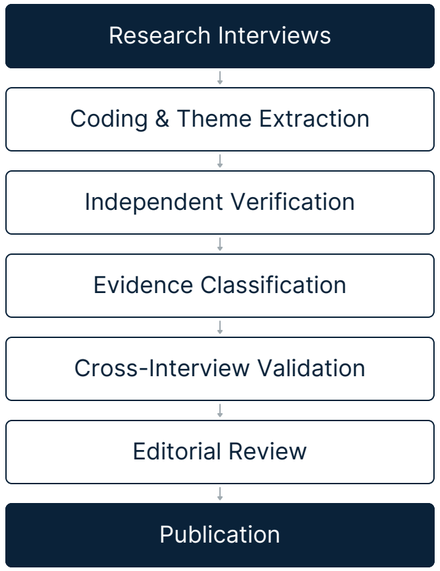
Across interviews with senior railway leaders, discussions rarely centred on cyber attacks alone. Instead, practitioners consistently described a broader organisational challenge — one where governance, operational continuity, interconnected systems and executive decision-making are becoming just as important as technical security controls.

Five strategic themes emerged — not as isolated concerns, but as an interconnected system where progress in one area depends on maturity in others.



How This Research Was Conducted

This report is based on structured interviews with senior railway leaders across seven European nations, conducted between January and May 2026. Participants included CISOs, CTOs, Operations Directors and Infrastructure Managers from both railway undertakings and infrastructure managers.



Editorial Principles

01 Evidence before opinion.

02 Observation before recommendation.

03 Practitioner experience over theory.

04 Transparency of evidence.

05 Continuous research.

PART ONE

The Railway is Changing

The convergence of operational technology, digitalisation and connectivity has fundamentally altered the risk landscape for European railways.

What is driving the change?

01 **Digitalisation**
Legacy analogue systems replaced by networked digital infrastructure at scale.

02 **Connectivity**
Previously isolated operational systems now interconnected and internet-accessible.

03 **ERTMS Deployment**
Standardised signalling introducing new digital interfaces across borders.

04 **Supply Chain Complexity**
Growing dependence on third-party technology providers and integrators.

05 **OT/IT Convergence**
Operational technology environments increasingly managed through IT networks.

What practitioners consistently described

> A shift in language — from 'cybersecurity' to 'operational resilience' — reflecting a broader understanding of what is actually at risk.

> Governance challenges that cross organisational boundaries, where accountability is unclear and decision-making is fragmented.

> A persistent gap between what leaders believe they can see across their operational estate and what they can actually observe in real time.

This research begins where traditional reports end.

What follows is not a list of threats.
It is what experienced practitioners told us about managing them.

FINDING 01

The Shift From Cybersecurity to Operational Resilience

Railway organisations across Europe are moving beyond a narrow focus on cybersecurity towards a broader conception of operational resilience — one that encompasses technology, people, processes and the complex interdependencies between them.

THIS FINDING EXPLORES

- The language shift from cybersecurity to resilience
- How organisations are reframing risk
- What operational continuity means in practice
- The implications for leadership and governance

FINDING 01 · PRACTITIONER EVIDENCE

Voices from the Research

> We stopped talking about cyber as a standalone thing. It is now part of how we think about keeping the railway running.
>
> — CISO, European Infrastructure Manager

> The board no longer asks 'are we secure?' They ask 'can we keep operating?' That is a fundamentally different question.
>
> — CTO, National Railway Undertaking

> Our incident response used to be about restoring systems. Now it is about maintaining service. The technology is secondary to the operational outcome.
>
> — Operations Director, Multi-modal Operator

> Our customers now ask us to demonstrate how our systems degrade gracefully. Five years ago they only asked if we met EN 50129.
>
> — Engineering Director, Signalling Manufacturer

> We are moving from prescriptive compliance to outcome-based assurance. The question is no longer 'did you patch?' but 'can you operate?'
>
> — Senior Inspector, National Safety Authority

RESEARCH FINDING

Operational resilience is replacing cybersecurity as the dominant executive conversation.

EVIDENCE STRENGTH

★★★★★

RESEARCH STATUS

Verified

CONFIDENCE

Very High

SUPPORTED BY

14 of 16 practitioners

CONFIRMING ROLES

Infrastructure Manager · CISO · CTO
Operations Director · Safety Authority
Signalling Manufacturer · Programme Director

RELATED

02 Governance · 04 Visibility · 05 Culture

Our interpretation

The shift from cybersecurity to operational resilience is not merely semantic. It represents a fundamental reframing of what organisations are trying to protect — from information assets to operational outcomes.

This reframing has profound implications. It moves accountability from the CISO's office to the executive team. It changes the metrics that matter — from vulnerability counts to recovery time objectives. And it demands a different kind of conversation at board level: one focused on business continuity rather than technical compliance.

Critically, organisations that have made this shift describe better alignment between security investment and operational priorities. Those that have not report persistent friction between security teams and operational leadership.

KEY INSIGHT

Organisations that reframe cyber as an operational resilience challenge — rather than a technical security problem — report stronger executive engagement and more coherent investment decisions.

Questions for your organisation

- Is cybersecurity still framed as a technical discipline in your organisation — or as an operational resilience challenge?
- Does your board discuss cyber risk in terms of system availability and service continuity — or in terms of vulnerabilities and compliance?
- Who is accountable for operational resilience when a cyber incident affects train operations?
- Can your organisation articulate what 'acceptable degradation' looks like during a cyber event?

CONFIDENCE LEVEL

HIGH

Consistent across 90%+ of interviews

SUPPORTING PRACTITIONERS

14 of 16 interviewees

RELATED FINDINGS

Finding 02: Governance
Finding 04: Visibility
Finding 05: Culture

NEXT → Finding 02: Governance Across Boundaries