# Rail Cybersecurity Summit 2027 Announces Ciaran Martin and Leading European Rail Cybersecurity Speakers

*Ciaran Martin CB joins rail leaders from NS, Bane NOR, Northern and regulators as AI, connected trains and digital dependency reshape rail cybersecurity.*



Delegates attend the Cyber Senate Rail Cybersecurity Summit in London.

LONDON, LONDON, UNITED KINGDOM, September 18, 2026 /EINPresswire.com/ -- Cyber Senate has announced the first speakers for the 13th Annual Rail Cybersecurity Summit, taking place in London on 9–10 March 2027, as railway organisations confront a new generation of cyber risk driven by artificial intelligence, connected rolling stock, software-defined infrastructure and growing dependency on external technology and supply chains.

The Summit will bring together senior leaders from rail operators, infrastructure managers, regulators, government and the cybersecurity community to examine how the industry can protect safety, resilience and operational continuity as railway systems become increasingly digital and connected.

> The question now is how rail organisations maintain safe and resilient operations when so much of the technology they depend upon is interconnected, externally managed or outside their direct control."
>
> *Jamison Nesbitt*

Opening the 2027 Summit will be Ciaran Martin CB, former founding CEO of the UK National Cyber Security Centre, who will examine the challenge of protecting critical infrastructure in an age of technological dependency.

Martin will be joined by senior speakers from across the European rail sector.

Dimitri van Zantvliet, Director Digital Resilience / CISO at Nederlandse Spoorwegen, will examine

the intersection between cybersecurity and artificial intelligence and how rail organisations should prepare for increasingly autonomous cyber threats.

Joseph Mager, Cyber Governance at Nederlandse Spoorwegen, will share early experience and lessons from the implementation of NIS2, examining what the new regulatory environment means for governance, accountability and cyber risk management.

From Norway, Tom Remberg, CISO at Bane NOR, together with Trond Eskild Tingstad-Stav from Traffic Management, will explore how Bane NOR is defining its Minimum Viable Company as part of building a defendable and resilient railway.

The session will examine how identifying the functions that must continue during major disruption can help organisations prioritise resilience, business continuity and cybersecurity investment.

Northern will address the increasingly complex cybersecurity boundary created by the connected train.

Its session, “The Connected Train: Who Controls the Data?”, will explore onboard connectivity, satellite and LEO communications, data sovereignty, encryption, supplier dependencies and the challenge of maintaining control when railway services increasingly depend on external networks and technology providers.



Ciaran Martin CB, former founding CEO of the UK National Cyber Security Centre, will open the 13th Annual Rail Cybersecurity Summit in London.



Delegates take part in an extended roundtable discussion at the Cyber Senate Rail Cybersecurity Summit in London.

From Germany, Dr Frank Werner of the Eisenbahn-Bundesamt (EBA) IT Security Taskforce will examine the relationship between railway safety oversight and cybersecurity, including European regulation, NIS2 and German critical-infrastructure requirements.

Senior representatives from the UK's Office of Rail and Road will also examine how software, operational technology and cyber risk are becoming part of the wider digital safety landscape.

Cybersecurity in a More Connected Railway

The 2027 programme will focus on the practical consequences of rail's accelerating digital transformation.

Key themes will include AI-enabled and autonomous cyber threats, connected rolling stock, data sovereignty, digital safety, NIS2, emerging regulation, supply-chain dependency, operational resilience, incident response, asset visibility, remote access and software-dependent railway systems.

Particular attention will be given to the changing boundary between railway operators and the technology ecosystems on which they depend.

From cloud platforms and remote connectivity to onboard systems, digital signalling, satellite communications and third-party software, railway operations increasingly rely on technologies and services beyond the traditional railway perimeter.

Jamison Nesbitt, Founder and Director of Cyber Senate, said:

“Rail cybersecurity has changed dramatically since we launched this Summit thirteen years ago.

“The conversation is no longer simply about protecting individual systems or meeting compliance requirements.

“The railway is becoming increasingly dependent on connected technologies, software, external service providers and complex supply chains, while AI is accelerating both the capabilities available to operators and the speed at which threats can evolve.

“The question now is how rail organisations maintain safe and resilient operations when so much of the technology they depend upon is interconnected, externally managed or outside their direct control.”

The Summit will continue Cyber Senate's format of expert presentations combined with extended operator-led roundtable discussions, giving participants the opportunity to compare approaches and explore how organisations are responding to common challenges in practice.

The 13th Annual Rail Cybersecurity Summit takes place on 9–10 March 2027 at The Cumberland Hotel, Marble Arch, London.

Further speakers and programme developments will be announced over the coming months.

Operational Risk Council will host the Roundtable Rail Supply Chain Forum

Cyber Senate's sister brand, "Operational Risk Council," wider rail programme also includes the Rail Supply Chain Roundtable Forum, taking place in London on 10 November 2026.

The Forum will bring together leaders from Network Rail, GBR Anglia, DfT Operator, East West Rail, Jacobs and other organisations to examine integration, supplier collaboration, engineering assurance, operational readiness and shared accountability across increasingly complex rail supply chains.

Ben Reed
The Cyber Senate
7522029376 ext.
email us here
Visit us on social media:
LinkedIn
Facebook

---

This press release can be viewed online at: https://www.einpresswire.com/article/943279695

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.