

Rail Cybersecurity Summit Returns to London for 13th Annual Edition

Delegate bookings are underway as the 2027 programme builds around rail cyber resilience, safety, regulation and operational security.

LONDON, UNITED KINGDOM, July 28, 2026 /EINPresswire.com/ -- The 13th Annual [Rail Cybersecurity Summit](#) will take place on 9-10 March 2027 at The Cumberland Hotel, Marble Arch, London, bringing together railway operators, infrastructure managers, rolling-stock organisations, regulators, government authorities, OEMs and cybersecurity specialists from across the international rail sector.

“

Attending Cyber Senate always reinvigorates my passion for cybersecurity and makes me want to go back to my company and shake things up again.”

*Rail Cybersecurity Summit
Attendee*

Now entering its thirteenth year, the Rail Cybersecurity Summit remains one of the longest-running specialist events dedicated exclusively to cybersecurity across railway operations, infrastructure, rolling stock and the

wider rail supply chain.

Delegate registrations for the 2027 summit are already underway, and organisers Cyber Senate are encouraging rail organisations currently allocating remaining 2026 cybersecurity, resilience, training and professional development budgets to secure participation early.

The 2027 programme is developing at a time when cybersecurity is becoming increasingly interconnected with railway safety, operational resilience, digitalisation, rolling-stock systems, supplier assurance and regulatory compliance.

Germany's National Safety Authority Joins the 2027 Programme

Among the latest organisations confirmed to contribute is Eisenbahn-Bundesamt (EBA), Germany's National Safety Authority, represented by Dr. Frank Werner of the EBA IT Security Taskforce.

Dr. Werner's contribution will examine the EBA's evolving role in integrating cybersecurity into railway safety oversight, including:

- EBA's developing role in connecting cybersecurity with railway safety supervision
- The responsibilities of the IT Security Department
- The legislative pathway from European laws and regulations into German law
- The implications of NIS2 and KRITIS for the rail sector
- Coordination with other German administrations and government ministries

The session will provide delegates with direct regulatory insight into how cybersecurity requirements are being incorporated into railway safety governance at both national and European level.

13TH ANNUAL

RAIL CYBERSECURITY SUMMIT

MARCH 9-10, 2027 **LONDON, UK**

OT SECURITY | NIS2 IMPLEMENTATION | THREAT DETECTION | REGULATION | INDUSTRY NETWORKING

WWW.RAILCYBERSECURITY.COM

13th Annual Rail Cybersecurity Summit, 9-10 March 2027, The Cumberland Hotel, Marble Arch, London.

Cybersecurity Is Becoming an Operational Rail Issue

The developing programme will address some of the most important cybersecurity and resilience challenges currently facing the railway sector, including OT security and operational resilience, cybersecurity and railway safety, AI in cybersecurity, vulnerability management, SOC development and threat detection, rolling-stock cybersecurity, supply-chain risk, secure procurement, NIS2, the EU Cyber Resilience Act, CLC/TS 50701, IEC 62443, governance and accountability, incident response, legacy systems, obsolescence, third-party risk, digital maintenance and secure remote access.

As railway environments become increasingly connected and software-driven, cybersecurity can no longer be treated purely as an IT concern.

Recent rail-sector research has highlighted how cyber compromise can potentially affect signalling, rolling stock, maintenance systems, operational information and even the processes used to identify or prevent unsafe conditions.

At the same time, rail authorities and operators are placing greater expectations on suppliers throughout the operational technology lifecycle, with increasing emphasis on secure development, vulnerability disclosure, patch management, software bills of materials, network segmentation, remote access, incident response, lifecycle support and supply-chain

accountability.

A Community Built Around Rail Cybersecurity

The Rail Cybersecurity Summit has always been designed around direct engagement between those responsible for operating, securing, regulating and supplying railway systems.

Its specialist focus allows delegates to discuss issues with peers who understand the particular challenges of protecting operational railway environments, where cybersecurity, safety, availability and long asset lifecycles must coexist.

One returning attendee commented:

"I find attending Cyber Senate always reinvigorates my passion for cybersecurity. Talking to others in the Railway OT world who are passionate and can see the need to do more in this space; technically, legislatively and in terms of training and recruitment makes me want to go back to my company and shake things up again to get us back into gear. I find I take more and more people not only from my team but from across my organisation each year."

Twelve Years of International Rail Participation

Across its previous editions, the Rail Cybersecurity Summit has welcomed representatives from railway operators, infrastructure managers, rolling-stock organisations, government bodies, regulators, OEMs, engineering organisations and cybersecurity specialists worldwide.

Past attendees include Network Rail, Transport for London, SNCF, SBB, Bane NOR, Deutsche Bahn, Irish Rail, Dutch Railways / NS, LNER, Northern, Transport for Wales, TransPennine Express, South Western Railway, West Midlands Trains, Copenhagen Metro, Metropolitan Transportation Authority, Land Transport Authority Singapore, CFL, SNCFL, STIB-MIVB, Sporveien, Angel Trains, Porterbrook, Eversholt Rail Group and Rock Rail.

Major rolling-stock, signalling, engineering and technology organisations represented have included Alstom, Siemens Mobility, Hitachi Rail, CAF, CAF Signalling, Stadler Rail, Thales, Knorr-Bremse, AtkinsRéalis, Systra, Televic GSP, Westermo, duagon, EKE-Electronics and ENYSE.

Government, regulatory and standards organisations attending previous editions have included Eisenbahn-Bundesamt, European Commission DG CONNECT, Office of Rail and Road, Rail Safety and Standards Board, Cyber Security Agency of Singapore, DfTO and the Human Environment and Transport Inspectorate.

The 2026 Rail Cybersecurity Summit was supported by Thales, Alstom, RazorSecure, Cylus, 4Secure, The Cyber Innovation Hub and GDAK.

Delegate Bookings for March 2027 Already Underway

Registrations for the March 2027 summit have already begun, with the event continuing to attract professionals responsible for cybersecurity, operational technology, engineering, digital transformation, signalling, rolling stock, risk, resilience and railway safety.

Organisations with remaining 2026 professional development, cybersecurity, resilience or training budgets are encouraged to register delegates during the current budget cycle rather than waiting until 2027.

The [early registration rate is £1,699 + VAT](#), with availability limited.

Delegate registration, sponsorship and exhibition opportunities will close once capacity is reached. The event is intentionally kept focused to preserve the quality of discussion, networking and engagement throughout the two days.

Rail Cybersecurity Summit 2027

9–10 March 2027

The Cumberland Hotel, Marble Arch, London, United Kingdom

<https://cybersenate.com/rail-cyber-security/>

Organisations interested in [sponsorship or exhibition opportunities](#) can contact marketing@cybersenate.com.

Ben Reed

The Cyber Senate

7522029376 ext.

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/929064488>

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.