Rail Delivery Group:
on track for cyber security

"Northdoor has helped RDG to cut business risk, improve cyber security, and ensure we embed best-practice, compliant policies."

Alan Cain, Head of Information Security,
Rail Delivery Group

- *Introduced enterprise protection for critical revenue and operational system*
- *Established governance and compliance for cyber security*
- *Reduced the business risk of service disruption and data breach*
- *Embedded best-practice cyber security for future operations*

About Rail Delivery Group

Rail Delivery Group (RDG) represents UK passenger and freight rail companies, Network Rail and High Speed 2. On behalf of its member companies, RDG is responsible for a host of shared services, including allocation and settlement of ticket revenue, discounted travel schemes, and third-party ticket sellers. RDG employs around 300 people.

At the buffers

Rail Delivery Group provides vital shared services to the rail industry. For example, RDG allocates revenue from tickets that span multiple train operating companies' franchises, and manages timetables across the UK.

The rail network provides essential services to the UK, from routine transport of food and goods to highly sensitive freight, such as nuclear waste. RDG and the train operating companies' operations routinely includes confidential data and personally identifiable information. With the global rise in pernicious hacks, particularly ransomware, RDG and its members take cyber security extremely seriously.

Ultimately, the core aim is to improve service reliability, reduce costs, and ensure rail safety. The greatest difficulty faced by RDG was gaining proper understanding of its third-party cyber-security risks, in order to be able to identify and remediate issues. With the complex mix of integrated systems and shared data across multiple RDG member train operating companies, how could RDG enhance cyber security across this very diverse data landscape?

On-time departure

RDG turned to Northdoor plc to deliver a strategic overview and propose ways to embed cyber security. This would include procurement assessments of multiple suppliers and service providers to the industry, the operational systems deployed in the industry, and better data protection for customers, stakeholders and RDG member companies.

At the recommendation of Northdoor, Rail Delivery Group chose to deploy the cloud-based RiskXchange, at RDG and at more than 40 member companies, to assess, monitor and manage third-party cyber risk across extended supply chains. The solution uses a combination of AI, machine learning, and rules engines to analyse and

"The net impact of working with Northdoor and implementing the RiskXchange solution will be better service reliability on UK railways, saving time and money for both RDG and its members, and improving freight and passenger rail services.."

Alan Cain, Head of Information Security, Rail Delivery Group

report in real time, replacing manual spreadsheets with an intuitive, live, dashboard. RiskXchange provides a simple, automated, and centralised risk management solution that enables RDG to manage and monitor its cyber risk score, and ensuring its suppliers, stakeholders and third-party partners meet its GDPR standards. For both RDG and the member companies, RiskXchange enables senior executives to manage risk in real time.

Alan Cain, Head of Information Security, Rail Delivery Group, comments, "RiskXchange enables us to gain enterprise-level insight into our cyber security risk and identify areas for remediation. Working with Northdoor we were able to rapidly implement and configure RiskXchange and establish essential policies and procedures as the foundation of a greatly improved cyber security posture."

Non-stop service

For a complex web of interconnected rail companies, onboarding new suppliers represents a specific and additional security risk. A new supplier to an individual train operating company is potentially gaining access to all RDG member companies' systems. Without central management, each train operator relied on every other company to manage and mitigate this risk.

With RiskXchange in place, RDG and its member companies enjoy a best-in-class third-party security framework. Assessments of procurement risk for suppliers are faster and more-effective, and all RDG members benefit from the improved, shared, cyber security stance.

Smooth running

The new RiskXchange solution has created a best-in-class cyber security framework for Rail Delivery Group and its member companies, offering a better, faster view of the cyber security risks they face. For example, the shared view of technology service providers that are common to multiple member companies places RDG a much stronger position to play an effective governance role. In turn, this helps to protect stakeholder investments, secure customer data, and to enhance the smooth and efficient running of rail services in the UK.

"Northdoor has helped RDG to cut business risk, improve cyber security, and ensure we embed best-practice, compliant policies," comments Alan Cain. "In addition, our cyber security is fully aligned with procurement, enabling faster and more-effective assessments of third-party risk during the onboarding of new suppliers."

Alan Cain concludes, "Most importantly, the net impact of working with Northdoor and implementing the RiskXchange solution will be better service reliability on UK railways, saving time and money for both RDG and its members, and improving freight and passenger rail services."