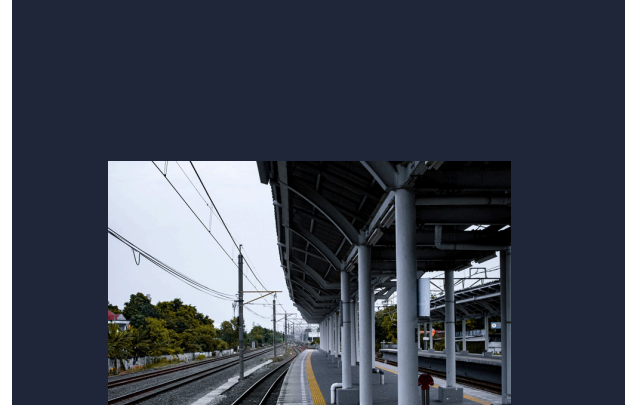


# RAIL DELIVERY GROUP

## CRITICAL INFRASTRUCTURE CASE STUDY

### RISKXCHANGE ESTABLISHES THIRD-PARTY GOVERNANCE & BUILDS A SECURE SUPPLY CHAIN



#### ABOUT THE COMPANY

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's routine operations include sharing confidential data and personally identifiable information with the train operating companies. With the complex mix of integrated systems and shared data across multiple RDG member train operating companies, RDG wants to enhance cybersecurity across this diverse data landscape.

#### CHALLENGES THE COMPANY FACED

##### Inefficient Third-party Risk Monitoring across the Extended Supply Chain

The greatest difficulty faced by RDG was gaining a proper understanding of its third-party cybersecurity risks to identify and remediate issues. With the extended supply chain of over 40 member companies, RDG struggled to assess, monitor and effectively manage third-party cyber risk via periodic assessments and audits, given that time is paramount for a national critical infrastructure organisation.

##### Insufficient Data Security

RDG wanted better data protection for customers, stakeholders and RDG member companies. The company shares sensitive data across multiple service and train companies, and with the global rise in pernicious hacks, particularly ransomware, RDG and its members needed to ensure their data is safe.

##### Lack of Third-party Security Framework & Central Third-party Management

For a complex web of interconnected rail companies, onboarding new suppliers represented a specific and additional security risk for RDG. 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.

#### HOW RISKXCHANGE SOLUTION HELPED

##### Continuous Third-party Risk Monitoring across the Extended Supply Chain

RiskXchange replaced RDG's manual spreadsheets with an intuitive, live dashboard. It provided a simple, automated, and centralised risk management solution that enabled RDG to manage and monitor its cyber risk score and ensure its suppliers, stakeholders, and third-party partners meet its GDPR standards. For both RDG and over 40 member companies, RiskXchange enabled senior executives to manage risk in real-time.

##### Improved Data Protection

RiskXchange enabled RDG to gain enterprise-level insight into their cyber security risk and identify areas for remediation. These helped RDG establish essential policies and procedures as the foundation of a greatly improved cybersecurity posture. RDG was able to build an environment for a more secure supply chain with the continuous assessment of their attack surface in real-time and instant alerts of the new cyber issues that could put their data at risk. With the help of the Dark Web Monitoring feature, RDG could ensure no company data has been leaked.

##### Central Third-party Management & Improved Third-party Governance

RiskXchange created an effective third-party security framework for RDG and its member companies, fully aligning their cybersecurity with procurement, enabling faster and more effective assessments of third-party risk during the onboarding of new suppliers, while the platform's AI assessment evidence scoring capabilities have streamlined risk assessment process for their current vendors.

The shared view of technology service providers common to multiple member companies placed RDG in a much stronger position to play an effective governance role. With RiskXchange, RDG built a comprehensive supply chain management process and created a preferred supplier list (PSL) to help the business and members choose the most secure vendor. Allowing RDG's suppliers to access the RiskXchange Platform themselves and see their risk scores enables them to remediate their issues, drive up their score, and get onto RDG's PSL.

“RiskXchange enables us to gain enterprise-level insight into our cyber security risk and identify areas for remediation. Our cyber security is fully aligned with procurement, enabling faster and more effective assessments of third-party risk during the onboarding of new suppliers...The net impact of 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 at Rail Delivery Group

