KPMG

The economic impact of a systemic cyber incident to the rail network

A KPMG report for the Department of Science, Innovation and Technology

April 2025

This research was supported by the Department for Science, Innovation & Technology and the R&D Science and Analysis Programme at the Department for Culture, Media & Sport. It was developed and produced according to the research team's hypotheses and methods. Any primary research, subsequent findings or recommendations do not represent Government views or policy.

Important notice

This Report has been prepared by KPMG LLP ("KPMG") solely for the Department of Culture, Media and Sport ("DCMS" or the "Client") in accordance with the terms of engagement agreed between DCMS and KPMG, dated 26th September 2024.

This Report is for the benefit of only the Client and the other parties (specifically the Department for Science, Innovation and Technology ("DSIT") that are included as beneficiaries of this research within the Agreement) that we have agreed in writing to treat as parties to the Agreement (together the "Beneficiaries").

This Report has not been designed to be of benefit to anyone except the Beneficiaries. In preparing this Report we have not taken into account the interests, needs or circumstances of anyone apart from the Beneficiaries, even though we may have been aware that others might read this Report. We have prepared this Report for the benefit of the Beneficiaries alone.

Please note that except as required by law, the Report is not intended to be copied, referred to or disclosed, in whole or in part. The Report is confidential. Any disclosure of the Report beyond the Beneficiaries may substantially prejudice KPMG LLP's commercial interests. If you receive a request for disclosure of the Report under the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002 we would ask that in accordance with recommended practice, you let us know and not make a disclosure in response to any such request without consulting us in advance and taking into account any representations made.

We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the Agreement.

This Report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the Beneficiaries) for any purpose or in any context. Any party other than the Beneficiaries that obtains access to this Report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through Beneficiary's Publication Scheme or otherwise) and chooses to rely on this Report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility or liability in respect of this Report to any party other than the Beneficiaries.

In particular, and without limiting the general statement above, since we have prepared this Report for the benefit of the Beneficiaries alone, this Report has not been prepared for the benefit of any other Government Department nor for any other person or organisation who might have an interest in the matters discussed in this Report.

Our work commenced on 26th September 2024 and our fieldwork was completed on 31st March 2025. We have not undertaken to update our Report for events or circumstances arising after that date.

Contents

List of abbreviations

Abbreviation	Definition
CISA	US Cybersecurity and Infrastructure Security Agency
CMM	Cancellation Minutes Multiplier
CNI	Critical National Infrastructure
DCMS	Department for Culture, Media and Sport
DfT	Department for Transport
DSIT	Department for Science, Innovation and Technology
ESRB	European Systemic Risk Board
ETCS	European Train Control System
GB	Great Britain
GBRTT	Great British Railways Transition Team
GDP	Gross domestic product
GVA	Gross value added
IID	KPMG's Industry Insights Database
IT	Information Technology
Mph	Miles per hour
NCSC	UK National Cyber Security Centre
NIS	Network and Information Systems
ONS	Office for National Statistics
ORR	Office of Rail and Road
OT	Operational Technology
REC	Railway emergency call
TAG	DfT's Transport Appraisal Guidance
UK	United Kingdom

Executive summary

Introduction to the study

As part of a wider programme of work to quantify the cost of cyber attacks to the UK economy, KPMG, with support from Professor Madeline Carr and Filippo Gualtiero Blancato from University College London (UCL), was commissioned by DCMS and DSIT to undertake research to improve the UK government's understanding of the economic harm of systemic cyber incidents[1], with a specific focus on the impact of systemic cyber attacks on the gas and rail networks.

This report sets out the findings in relation to the scenario of a systemic cyber incident on Great Britain's (GB) rail network. The specific scenario the assessment was based on was developed in conjunction with DSIT and the Department for Transport (DfT). The scenario is intended to represent a 'reasonable worst-case scenario'[2]. It should be noted that this is a hypothetical scenario and not a prediction. An assumption-driven approach to the modelling has therefore been adopted and results presented in this study should be considered as indicative only.

Below is the summary description of the systemic cyber incident on the rail network. The full scenario and details of the specific parameters used for modelling purposes are in Section 1.2 of the report.

The scenario focuses on a cyber incident involving a trains communications system operated by Network Rail. In the scenario, a cyber attack on the trains communications system leads to a system degradation over a short period of time before the total loss of the service resulting in a loss of the trains communications system across the entire rail network. As a result, certain lines that rely on the system[3] will immediately cease operating until the system is restored. For four hours, all services can operate at line speeds up to 100 miles per hour (mph) after which speeds must be reduced to 60mph until the trains communication system service is restored. This will result in delays and cancellations across the network. For the purposes of this scenario, it has been assumed that rail services would be disrupted for one week.

In the development of the study, a number of approaches were used to collect evidence and understand the potential impact of a systemic cyber incident, including a systematic literature review; impact mapping to identify impacts and prioritise those to be included in the modelling; and data collection from DfT and Network Rail, as well as public data sources to inform appropriate modelling of cost to the UK economy of a cyber incident on the rail network and qualitative assessment of impacts.

An overview of the approach taken to model the economic costs associated with the scenario is provided in Section 5.

Summary of the economic impacts of a systemic cyber incident to the rail network

In the study, the quantitative analysis of the potential impact of a systemic cyber incident considers two broad types of impact:

[1] The Department for Science, Innovation and Technology (DSIT) define a systemic incident as one which will have a large impact on the economy either because: (1) an organisation that is a piece of critical national infrastructure (CNI)[1] has been compromised resulting in their supply chain suffering with a reduction in capacity to operate; or (2) a wide-spread attack affects many firms, organisations or individual at the same time, causing the firms to experience an inability to use their digital systems.
[2] A reasonable worst-case scenario is a generic representation of a challenging yet plausible manifestation of a risk.
[3] Those that use Level 2 European Train Control System.

— the direct impact, relating to the direct financial cost to the organisation that is subject to the cyber attack; and

— the indirect economic impacts, capturing the impacts on train and freight operators, passengers and consumers, businesses and the wider economy.

In total, it is estimated that the systemic cyber incident to the rail network could result in a total economic cost of approximately £1.8 Billion for a weeks period of disruption. It is estimated that the hypothetical systemic cyber incident to the rail network could result in a direct financial cost to Network Rail in the region of £123.0 million, a cost to passengers of delays of £281.3 million and a potential impact on gross value added (GVA)[4] of up to £1,397.0 million. This total estimated GVA impact is largely comprised of lost output due to the impact of freight disruption on production and the wider economic impacts through the supply chain of this disruption and of the direct impact on freight and rail sector output. While train and freight operators are expected to be affected by the cyber attack through loss of revenues, their contracts with Network Rail mean that they would be compensated for any losses by Network Rail – the costs of which are included in Network Rail's direct financial costs. Put in context, the estimated GVA impact represents approximately 2.8% of the UK's total GDP per week, and 0.05% of annual GDP.

It is noted that the approach applied to modelling the lost output due to the impact of freight disruption on supply chains assumes that the reduction in key inputs to production results in a proportionate reduction in output for the sectors most impacted (namely 'Construction', 'Manufacture of cement, lime, plaster and articles of concrete, cement and plaster' and 'Manufacture of glass, refractory, clay, porcelain, ceramic, stone products'). In practice some substitution between inputs to production is likely to be possible, which would reduce this impact.

Table 1 below presents a summary of the direct and indirect economic impacts of a systemic cyber incident to the rail network under the reasonable worst-case scenario analysed.

[4] GVA is a measure of the economic value of the goods and services produced at an individual company, industry or sector level, net of intermediate consumption (i.e. the goods and services that are used in the production process). GVA estimates the difference between the value of goods and services produced and the cost of inputs, such as unprocessed materials, used to create those goods and services. A nation's GDP includes the sum of the GVA of all economic agents within the economy.

Table 1: Summary of the direct and indirect economic impacts of a systemic cyber incident to the rail network

Impact type	Stakeholder impacted	Impact area	Estimated economic impact (£ million, 2024 prices)
Direct	Network Rail	Direct financial cost to organisation (a)	£123.5
Indirect	Train and freight operators[5]	Cost of lost output (GVA) (b)	£0
	Passengers/consumers	Cost of longer journey times (c)	£281.3
	Businesses	Productivity impact of lost work days (GVA) (d)	£116.7
		Cost of lost output due to supply chain (freight) disruption (GVA) (e)	£520.1[6]
Wider economic impacts		Wider supply chain impact of reduction in output (GVA) (f)	£760.1
Total GVA impact (excludes consumer impacts, therefore equal to b, d, e, f)		The productivity impact of lost work days, cost of lost output due to supply chain disruption and wider supply chain impact.	£1,397.0
Total Economic Cost (a,b,c,d,e,f)			£1,801.7

Source: KPMG analysis

In addition to the impacts that have been monetised, there are further potential indirect economic impacts that have not been captured within the analysis but have been considered qualitatively. These impacts are summarised in Table 2 below.

Table 2: Summary of the qualitative assessment of indirect and wider economic impacts of a systemic incident to the rail network

Impact	Summary
Impacts on passengers/consumers	
Impact of forgone rail journeys	— Service disruption is expected to result in train cancellations and delays. Based on the impact of Storm Eunice[7] on train services, a 53% reduction in the number of trains running each day is assumed. — The number of passenger journeys is expected to fall by approximately a third. [8] Those unable to travel will include those intending to travel for work/commuting, to or from education or for leisure. [9] While many workers can work from home or change their work hours days, a minority would be expected to have to reduce the number of hours worked or not work at all – resulting in a loss of earnings (reflected in the quantified productivity impact).[10] — Reduction in travel for education or leisure purposes may also result in a welfare cost for those affected.

[5] While train and freight operators are expected to be affected by the cyber attack through loss of revenues, their contracts with Network Rail mean that they would be compensated for any losses by Network Rail – the costs of which are included in Network Rail's direct financial costs.
[6] Ibid.
[7] Storm Eunice affected the UK in February 2022, bringing severe weather that resulted in major disruption and widespread line closures to the rail network. The impact of Storm Eunice on rail services is used in this study as a proxy for the disruption caused by the cyber incident scenario.
[8] Assumption provided by Network Rail based on evidence from Storm Eunice.
[9] DfT (2024) National Travel Survey
[10] DfT (2023) Rail strikes: Understanding the impact on passengers – full report. Note, respondents could select multiple response.

Impacts on wider consumers	— Among those that no longer travel by rail, it is expected that approximately one third would make their journey by alternative modes of transport – largely private vehicles or bus. [11] — Mode shift will result in increased congestion on the roads, increased pressure on all public transport systems and potentially longer journey times for all those travelling.
Impact on passenger safety	— The cyber incident would cause a limited number of rail lines to immediately cease operating, leaving passengers on these lines stranded. This would be manged by Network Rail through standard procedures[12], though nonetheless, could generate some additional risk to passenger health, safety and security. — Crowding at stations due to lower throughput of trains may have some impact on passenger safety, though this is expected to be limited. [13,14]
Impacts on businesses	
Impact of reduced footfall/ consumer spending	— Reduced travel would be expected to reduce retail, hospitality and leisure footfall and impact consumer spending during the period of disruption.[15] — While some individual businesses may experience loss of revenues as a result (with convenience food and drink outlets likely to be most heavily affected), consumer spending would be expected to be largely diverted e.g. to online or local suppliers, or delayed to a later date. [16]
Impact of supply chain disruptions	— Disruption to rail freight will have a knock on impact on supply chains across the UK. — Intermodal freight makes up the largest share of rail freight by volume lifted. [17] Some of this would be able to be diverted to road, though this would generate additional financial costs, increased congestion and likely delays. Furthermore, it is expected that some substitution would be possible across many intermodal freight products, meaning that rather than leading to significant shortages or impacts on production, reduced consumer choice is more likely. — The most heavily impacted sector is expected to be the construction sector, with construction products making up a third of all rail freight by volume lift. [18] Disruption to construction supplies could have a short term impact on construction sector output. This is covered in the quantitative analysis. — Disruption to the movement of intermodal maritime freight would be expected to have knock on impacts on ports, if onward movement of goods is impacted, with potential subsequent impacts on international trade.

Source: KPMG analysis

The study finds that systemic cyber attacks on Critical National Infrastructure (CNI) can generate similar types of impacts as conventional attacks that result in disruption to infrastructure. What distinguishes cyber attacks is their scalability, replicability and relatively low cost nature, meaning the impacts realised can be much larger and more widespread at limited additional cost to the perpetrator. Nonetheless, there are some potential specific costs of cyber attacks over and above those linked to conventional attacks, including financial costs of malware and data breaches. Costs of such data breaches can go beyond financial loss. If, as could be the case in a cyber attack on CNI, sensitive operational information (e.g. nuclear information, routes, dangerous freight loads etc) is lost, this could result in more substantial risks in terms of safety and national security. It is noted that, given

[11] DfT (2023) Rail strikes: Understanding the impact on passengers – full report. Note, respondents could select multiple response.
[12] Network Rail & Rail Delivery Group (2020) RDG and Network Rail Guidance Note: Meeting the Needs of Passengers Stranded on Trains
[13] ORR (2024) ORR's health and safety crowding position statement
[14] Ibid.
[15] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[16] ONS, 2023. The impact of strikes in the UK - Office for National Statistics
[17] ORR, 2025 Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal
[18] ORR, 2025 Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal

the parameters of the scenario considered for the study, such costs resulting from data loss are not considered within the study.

Summary of the assessment of the likelihood of a systemic cyber incident to the rail sector

For this likelihood assessment of a systemic cyber incident impacting the UK rail sector, the risk of a malicious threat actor conducting a successful attack, is balanced against an assessment of the vulnerability potential targets are to an attack, amplification factors, as well as institutional, legal and regulatory countermeasures in place. These 4 parameters, informed by the qualitative assessments and insights in Section 6.3, are collated together to form one likelihood assessment. Evidence mapped against four phases of the European Systemic Risk Board (ESRB) framework for assessing systemic cyber risk[19] leads to an assessment that there is a low likelihood that within a 2 year period a cyber incident targeting the UK rail sector will result in systemic level impact leading to significant disruption of rail services.

Recent incidents in the UK and Europe show that one of the most common assets targeted in the rail sector are ticketing systems. These incidents however have an isolated financial impact on victim organisations as factors leading to systemic event are not present. In war zones such as Ukraine and Russia, rail service providers are targeted by state sponsored groups and hacktivists seeking to gain political capital and disrupt operations. It is unlikely the UK rail network is a target of these groups, but this status could change with evolving geopolitical events in Europe, and globally.

The widespread impact of recent incidents has been mitigated by security controls and cyber maturity of organisations in the rail sector as well as national level policies promoting cybersecurity practices such as regulatory enforcement, information sharing and education. It is important to note that cybersecurity maturity is not consistent across the sector and there remains a risk an incident could occur in a single organisation and spread to other organisations. Further, this assessment should be reviewed over time as changes to the threat landscape occur. As such, continued monitoring of the above factors is recommended to ensure the likelihood scoring remains accurate for future assessments.

[19] ESRB (2020) Systemic Cyber Risk.

1 About the study

1.1 Introduction to the study

The UK Government Department for Culture, Media and Sport (DCMS) is running a Research & Development Science and Analysis Programme across DCMS and the Department for Science, Innovation and Technology (DSIT). The Programme is focused on delivering longer term (3-5-10 years in the future), more cross-cutting, and more experimental approaches to research than traditional methods of evidence development within the Department.

One area of work under this Programme relates to quantifying of the cost of cyber attacks to the UK economy. Quantifying the cost of cyber attacks to the economy is a challenging exercise, and is currently without an established, consensus methodology. To demonstrate the importance and urgency of enhancing the UK's cyber resilience and capabilities, the UK Government is looking to develop a robust and comprehensive methodology to estimate the economic impact of cyber attacks on the UK.[20]

To support this programme of work, KPMG, with support from Professor Madeline Carr and Filippo Gualtiero Blancato from University College London (UCL), was commissioned by DCMS and DSIT to undertake research to improve the UK Government's understanding of the economic harm of systemic cyber incidents[21], with a specific focus on the impact of systemic cyber attacks on the gas and rail networks.

This report sets out the findings in relation to the scenario of a systemic cyber incident on Great Britain's (GB) rail network.

At the inception of this study, a series of research questions that this study should help answer were agreed between KPMG and DCMS/DSIT. These are as follows:

1) What are the specific impacts if the critical sector is victim to a cyber attack compared to a conventional (physical) attack?

2) Where are the economic impacts felt across businesses and consumers?

3) What are the economic costs of the attack? This includes both direct (e.g. immediate financial losses and recovery costs); and indirect costs (e.g. those resulting from reduced investments; and reduced consumer confidence in the sector).

4) What is the best methodology to model such an attack?

5) What is the perceived probability of the attack occurring?

6) Does the scenario of a cyber attack challenge current assumptions on the impact and recovery of the sector compared to conventional attacks?

[20] Department for Culture, Media & Sport (2024) Invitation to Tender (ITT) For: Contract for services: R&D Science and Analysis Programme – Economic Modelling of Cyber Systemic Incidents.
[21] The Department for Science, Innovation and Technology (DSIT) define a systemic incident as one which will have a large impact on the economy either because: (1) an organisation that is a piece of critical national infrastructure (CNI)[21] has been compromised resulting in their supply chain suffering with a reduction in capacity to operate; or (2) a wide-spread attack affects many firms, organisations or individual at the same time, causing the firms to experience an inability to use their digital systems.

7) Does the scenario of a cyber attack challenge the current assumptions on the impacts felt across other CNI (critical national infrastructure) sectors, wider sectors, businesses and consumers?

It is noted that, with reference to research questions 6 and 7, given a lack of available detail in relation to the assumptions held by Government in relation to conventional attacks, discussion with DSIT at the outset of the study identified that the report should support DSIT's own understanding in relation to these questions, rather than answer these questions explicitly.

1.2 Overview of the systemic cyber incident scenario on the GB rail network

In this study, assessment of the economic costs of a systemic cyber attack on the rail network is based on a specific cyber incident scenario. This scenario has been developed in conjunction with DSIT, the Department for Transport (DfT) and Network Rail. The scenario is intended to represent a 'reasonable worst-case scenario'[22]. It should be noted that this is a hypothetical scenario and not a prediction. Within the scenario, it has been assumed that certain actions would be taken by Government departments and/or other organisations in response to the cyber incident. Unless otherwise stated these do not reflect official UK Government policy or plans. With this in mind, and given the hypothetical nature of the scenario, assessment of the potential economic costs in such an event should be considered as indicative only.

Below is the summary description of the systemic cyber incident on the rail network.

The scenario focuses on a cyber incident involving a trains communications system operated by Network Rail. The trains communications system is used for voice communication between signallers and drivers, including for the railway emergency call (REC) which stops all trains in the vicinity and for the European Train Control System (ETCS) – the new generation of digital signalling that uses the radio network as a bearer. In the scenario, a cyber attack on the trains communications system leads to a system degradation over a short period of time before the total loss of the service resulting in a loss of the trains communications system across the entire rail network.

As a consequence of the cyber incident, the following events and outcomes are expected:

- Communication between signallers and driver via the trains communications system will cease whilst the network is down.[23]
- Safety functions like the REC button will not be able to operate.
- Lines utilising Level 2 ETCS[24] without the availability of trackside signalling will immediately be stopped and cannot operate until the network is restored.
- As per the Rail Industry Standard (RIS3780) which covers this scenario, for four hours services can operate at line speeds up to 100 miles per hour (mph) after which speeds must be reduced to 60mph until the trains communications system service is restored.
- Recovery of the trains communications system from the cyber incident is anticipated to take a maximum of a week. For the purposes of this scenario, it has been assumed that rail services would be disrupted for one week.

Full details of parameters and assumptions applied in the analysis can be found in Sections 4 and 5.

[22] A reasonable worst-case scenario is a generic representation of a challenging yet plausible manifestation of a risk.
[23] During this time normal mobile phones can be used or if no mobile signal is available there are trackside Signal Post Telephones at each signal that can be used, but would slow operation.
[24] ETCS Level 2 is a radio-based signalling system that displays signalling and movement authorities in the cab, eliminating the need for lineside signals.

1.3 Overview of the scope and approach to the research and analysis

1.3.1 Scope of the study

In the analysis of the potential impact of a systemic cyber incident, two broad types of impact are considered:

1) The direct impact of a systemic cyber incident on the rail network, referring to the direct financial cost to the organisation that is subject to the cyber attack. These typically include, as relevant, costs such as productivity costs of operational disruption; incident response costs; costs of system recovery and replacement of any damaged capital assets; and costs of any fines issued as a result of the cyber security failings. Direct impacts are assessed quantitatively using the Open FAIR™ risk analysis[25] framework. Details on the approach to assessing the direct impact is provided in Section 4.

2) The indirect economic impacts, including:

   a) Impacts on train and freight operators using the rail network.

   b) Impacts on passengers directly impacted by disruption to the rail network, e.g. lost journeys or longer journey times and wider consumers.

   c) Indirect impacts on businesses resulting from behavioural changes in response to the disruption of rail services, e.g. lost productivity and/or output from workforce and supply chain disruption.

   d) Wider economic impacts realised across the economy (in terms of GVA[26]) across the UK supply-chain).

   The indirect impacts have been assessed using a combination of bespoke analysis and Input-Output modelling. Detail on these approaches and how they have been used is provided in Section 5. Where impacts are not modelled quantitatively, they are assessed qualitatively based on available data, literature and economic theory.

The report also considers the likelihood of such an attack occurring. Specifically, a high-level qualitative assessment of systemic risk in the rail sector is conducted drawing on the European Systemic Risk Board (ESRB) framework for assessing systemic cyber risk.[27] Detail on how the likelihood assessment was conducted is provided in Section 6.

The study assesses the potential impact on the UK economy of the scenario. It is noted that in the scenario the attack is on the GB rail network and there is not expected to be any direct or second-order impacts on the Northern Ireland rail network. However, to the extent that freight is disrupted due to the cyber incident, there may be some impact on supply chains in Northern Ireland.

1.3.2 Summary of approach

In the development of the study, a number of approaches were used to collect evidence and understand the potential impact of a systemic cyber incident, as follows:

[25] Open FAIR™ risk analysis is a risk management framework for breaking down the factors that contribute to risk and how they affect each other. It provides a taxonomy for deconstructing the likelihood and impact from loss events.
[26] GVA is a measure of the economic value of the goods and services produced at an individual company, industry or sector level, net of intermediate consumption (i.e. the goods and services that are used in the production process). GVA estimates the difference between the value of goods and services produced and the cost of inputs, such as unprocessed materials, used to create those goods and services. A nation's GDP includes the sum of the GVA of all economic agents within the economy.
[27] ESRB (2020) Systemic Cyber Risk.

— Systematic literature review to gather existing evidence of the impact of systemic cyber incidents.

— Impact mapping to identify potential areas of impact to be assessed, including prioritisation of impacts for inclusion in the economy modelling.

— Data collection and analysis, drawing on data from public sources as well as data provided by DfT and Network Rail to inform appropriate modelling of cost to the UK economy of a cyber incident on the rail network and support qualitative assessment of impacts.

Detail on each of these steps and the approach taken is provided in the sections below.

1.3.3 Systematic literature review

A systematic literature review was undertaken by Professor Madeline Carr and Filippo Gualtiero Blancato from UCL to gather relevant evidence on the socio-economic impact of cyber incident on Critical National Infrastructure (CNI). The literature review covers existing research on the impact of cyber-related incidents on critical infrastructure. At the outset of the study, a literature review protocol was developed by academics at UCL to set the parameters of the systematic review. The literature review protocol is set out in Appendix 1.

The literature review drew upon peer-reviewed academic studies and grey literature, such as working papers, industry reports, technical analyses and international organisations' research. The studies reviewed cover a wide range of geographies but in many instances findings can be transferred to the context of the UK economy.

The literature review was used to identify the types of economic impacts CNI cyber incidents have previously generated and how they have been measured, to inform the scope and approach to analysis and modelling for this study. Where relevant to the scenario, these findings have been drawn upon in the qualitative assessment of potential impacts as well as in the quantitative modelling of the economic impacts.

1.3.4 Mapping of impacts

In considering the specific scenario of a systemic cyber incident on the rail network, impact mapping was used to understand the routes through which economic costs may be realised and any dependencies or specific conditions that may be relevant to these. The impact map is used to detail the potential outcomes and impacts that may arise as a result of a systemic cyber incident to the rail network. It shows the causal link between stages of the theory of change and helps support the attribution to the end impact on the UK economy, at least in part, back to the initial shock of the systemic cyber incident. The resulting impact map is presented in Section 3 of this report.

The impact map was developed following engagement with stakeholders from DSIT, DfT and Network Rail to better understand the parameters of the scenario and how different economic agents may respond. In addition, the impact map reflects insights and findings from the literature review on the types of impacts that may be realised, or would be expected to be realised, following a cyber incident on the rail network.

The impact mapping identified a long-list of possible impacts from the scenario. From this, impacts were prioritised for inclusion in the modelling based on the principles of materiality of impact, proportionality (in terms of ease of modelling and potential scale of impact) and the ability to robustly model the impact e.g. in terms of data/evidence availability. This prioritisation was informed by insights drawn from the literature review, a data and evidence review and engagement and consultation with DSIT, DfT and Network Rail.

This process was used to determine the list of impacts to be taken forward to modelling. Other impacts identified, but not prioritised for quantitative assessment were assessed qualitatively, drawing on findings from the literature review, economic theory and consultation with DfT and Network Rail.

1.3.5 Data collection and analysis

In the modelling of the economic impacts of a systemic cyber incident on the rail network, a number of data sources were used. Where possible, data was taken from publicly available sources such as the Office for National Statistics (ONS) and other government departments.

It is noted that, given the novel nature of the scenario being considered, there is limited appropriate data or forecasts to draw upon when assessing the potential economic impact of the cyber incident. In this context, and through consultation with DfT and Network Rail, data from Network Rail on the level of disruption and impacts from Storm Eunice[28] in 2022 has been used as a useful proxy for the scale of impacts of the cyber attack scenario.

In addition to data on the impact of Storm Eunice, the analysis of the potential economic impact of systemic cyber incident on the rail network draws on the following key sources of data:

- KPMG's Industry Insights Database (IID).[29]
- Data on rail use, passenger numbers and freight volumes including Office of Rail and Road (ORR) data on total passenger journeys[30] and the National Travel Survey.[31]
- Data and information from a DfT survey of passengers affected by rail strikes over the summer and early autumn of 2022.[32]
- National economic indicators, including data on GVA and economic output by sectors sourced from the ONS.[33, 34]
- Input-Output[35] and Supply and Use tables[36] sourced from the ONS.

Where data could not be sourced from public sources or through stakeholders, assumptions were applied in the modelling. These assumptions were developed based on wider available literature and/or developed in consultation with DSIT, DfT and Network Rail. Where broader assumptions have been applied, the impacts should be considered as indicative rather than precise estimates.

All results are presented in 2024 prices.

[28] Storm Eunice affected the UK in February 2022, bringing severe weather that resulted in major disruption and widespread line closures to the rail network.
[29] KPMG's IID is a database of expected costs for organisations from cyber attacks. It contains approximately 1500 individual datapoints on the costs of cyber attacks, typically covering response and recovery costs. Data for these costs derive from several sources including: industry publications such as Cyentia's IRIS; other publicly available sources like press reports; and data and evidence gathered through KPMG's internal Cyber Response Services team.
[30] ORR (2024) Passenger rail usage; ORR (2024) Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal
[31] DfT (2024) National Travel Survey
[32] DfT (2023) Rail strikes: Understanding the impact on passengers – full report
[33] ONS (2024) Annual Business Survey (ABS) – Non-financial business economy, UK: Sections A to S' [Published 8th April 2024]
[34] ONS (2024) Monthly Business Survey turnover in production industries [published 15th November 2024]
[35] ONS (2022) Input-Output analytical tables - Office for National Statistics
[36] The estimated reduction in intermediate demand for construction products is distributed proportionately across sectors based on their relative intermediate demand for these products. The associated of reduction total intermediate demand in each sector is then estimated based on the value of reduction of consumption of construction products as a proportion of total intermediate consumption. It is assumed that the change in GVA for each sector is proportionate to the change in intermediate consumption. This is a simplifying assumption, but allows for an estimation of the indicative scale of impact.

Details of the analytical assumptions and data sources used in the development of this study are included in Sections 4 and 5 alongside full details of the modelling approaches used.

1.4 Report structure

The remainder of the report is structured as follows:

- Section 2 sets out the key evidence and findings from the literature review, including relating to the potential threat and nature of cyber incidents; the potential impacts of a systemic cyber attack; existing evidence on the economic costs of a systemic cyber attack and the methodologies that have previously been used to measure these.
- Section 3 presents the impact map developed to show the potential flow of economic impacts of the systemic cyber attack through different stakeholders and through the economy.
- Section 4 sets out findings of the assessment of the direct financial cost of a systemic cyber incident to the organisation that is subject to the attack.
- Section 5 sets out findings of the assessment of the indirect economic impacts of a systemic cyber incident to the rail network on wider stakeholders. This includes an assessment of:
  - economic impacts to train and freight operators (5.2)
  - economic impacts to GB passengers/consumers (Section 5.3)
  - economic impacts to UK businesses (Section 5.4)
  - wider economic costs of a rail cyber incident through the UK supply chain (Section 5.5).
- Section 6 provides an assessment of the likelihood of a systemic cyber incident to the rail network in the UK.
- Appendix 1 presents the literature review protocol developed at the outset of this study.
- Appendix 2 includes the detailed findings of the literature review undertaken by UCL.
- Appendix 3 provides details of the approach to the analysis undertaken and the specific methodologies and assumptions that have been applied in the modelling.

2 Evidence from the literature review of systemic cyber incidents

2.1 Introduction to the literature review

A systematic literature review was conducted on the socioeconomic impact of cyber incidents on CNI. At the outset of the study, a literature review protocol was developed by academics at UCL. The literature review protocol is set out in Appendix 1.

The literature review includes studies that analyse cyber-related incidents and attacks on critical sectors of the economy such as rail transport, oil and gas, the power grid, seaports, and cloud infrastructures. Whilst these sectors have their own specificities, attacks on these sectors follow similar dynamics and some commonality in terms of the types of economic impacts that occur. In total 21 academic studies and 10 sources of grey literature, including Government papers and industry reports, were reviewed. These provide a comprehensive and robust view of the nature of impacts of cyber attacks across CNI.

It is noted however, that studies covered by the literature review include examples from a range CNI, and across different countries and scenarios. All findings should therefore be considered indicative, rather than being specific to the scenario under consideration in the study.

The following sections set out the key findings from the literature review aligned to key research questions posed as part of this study. A detailed write-up of the literature review can be found in Appendix 2.

2.2 Summary literature review findings

2.2.1 The potential threat and nature of cyber incidents on critical infrastructure

Research question 1: What are the specific impacts if the critical sector is victim to a cyber attack compared to a conventional attack?

In general, the literature reviewed suggests that there are increasing threats of cyber attacks on CNI. Over recent years, cyber attacks have become increasingly sophisticated with different configuration types, such as ransomware, malware, manipulation methods, phishing and spear-phishing.[37] Technological advancements in, and the widespread adoption of, information and communication technologies in infrastructure has meant that the threat of cyber attacks is greater and the potential impact more severe.[38] Further, the integration of industrial control systems within CNI and 'industrial networks'[39] means that these systems are increasingly being targeted by malicious actors such as hackers, industrial spies and even foreign armies and intelligence agencies.[40] Additionally, the literature identifies that the continued use of legacy systems, specifically in the rail network, can

[37] Kendzierskyj, S and Jahankhani, H (2019) The Role of Blockchain in Supporting Critical National Infrastructure, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 208-212.
[38] Kour, R; Karim, R; Thaduri, A (2020) Cybersecurity for railways – A maturity model. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit; 234(10):1129-1148.
[39] This refers to legacy networks established within CNI and typically replicated and adopted across CNI sectors. Most CNI now uses a matrix of off the shelf solutions on their own industrial networks. It is the integration of industrial controls systems and off the shelf products on the industrial networks of CNI that leads to them being more vulnerable and targeted.
[40] Pricop, E; Mihalache, SF, (2015) Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems. 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania.

increase vulnerability to cyber threats as these systems are not designed to protect against modern cyber threats.[41]

Cyber attacks on CNI generally were found to pose a particular kind of threat over and above conventional attacks on physical infrastructure. Cyber attacks can easily spread through infrastructure, especially in the age of the industrial internet of things, thereby magnifying the damage compared to what a conventional attack would achieve. Moreover, cyber attacks can be more easily repeated (e.g. attackers coordinating bots to launch several strikes to overwhelm traffic or disrupt a network component), which means that recovery from cyber-related disruptions can take longer to recover from and requires a great deal of coordination from the defenders. From this perspective, cyber attacks are a low cost option for threat actors and can be difficult to attribute, meaning they are lower risk for the perpetrator.

In terms of the nature of the impacts of cyber attacks, many of the types of the impacts of cyber attacks will align to the types of impacts from conventional attacks, or wider sources of network disruption. However, there are additional potential impacts from cyber attacks specifically. These include financial costs resulting from ransomware or data breaches.[42] Furthermore, the impact of data loss can be substantial if sensitive operational information (e.g. nuclear information, routes, dangerous freight loads etc) is lost, which can result in more substantial risks in terms of safety and national security.

2.2.2 Identified impacts of a systemic cyber incidents on critical infrastructure

Research question 2: Where are the economic impacts felt across businesses and consumers?

The following sub-sections present summary findings from the literature review in relation to the impact on business, consumers and the wider economy in turn.

Impacts on businesses

The literature suggests that cyber incidents can increase costs and reduce revenue for the businesses/organisation targeted through a cyber incident. Specifically, studies show that cyber incidents can:

- Generate high costs for businesses in the short-term as businesses may experience shutdowns or equipment failure and may need to repair damaged assets.[43]
- Damage the reputation of affected business(es) impacting revenues and, when if publicly traded, stock performance. For example, the CrowdStrike incident in July 2024 resulted in a significant fall in the firm's share price of 22.9% between 18 to 24 July 2024, representing a change in market cap of around USD19 billion.[44,45, 46]

There is a distinction between the impacts on the businesses that were targeted through cyber incidents and those that experience second-order impacts as a result of the systemic nature of the cyber incident. Examples of second-order impacts on businesses from cyber incidents to CNI include:

[41] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science
[42] James E. Lerums, J. Eric Dietz, (2018). The Economics of Critical Infrastructure Controls Systems' Cyber Security. IEEE International Symposium on Technologies for Homeland Security (HST)
[43] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[44] KOVRR (2024) The UK Cost of the CrowdStrike Incident.
[45] Revenue impacts and stock performance is only relevant where CNI is owned and operated by a private business. In some instances CNI may owned and operated by public sector organisations, in which case these would apply. There would, however, be disruption to operations and a financial cost resulting from a cyber incident.
[46] It is noted, however, that the impact on the reputation and stock price of CrowdStrike may be particularly high given that CrowdStrike operates in cybersecurity and is not necessarily typical of incidents in other sectors.

— Disruption to operations either due to loss of service (e.g. power cuts) or through the upstream supply chain (e.g. as a result of disruptions freight transported via railways). In some instances this can lead to business closure.[47] Such disruptions to business operations may result in a loss of revenue for businesses affected.
— A reduction in workforce productivity, for example as a consequence of travel disruption employees unable to travel to work. One study estimated that a cyber incident on the electricity grid in the UK could result in the disruption of more than 800,000 individual train journeys per day in areas affected by the power failure, and that this could contribute (along with other factors) to a 50% reduction in labour productivity.[48] Another study estimated that a cyber incident to the US electric grid could cause a 10-60% attrition in the workforce across supply chain sectors.[49]

Impacts on consumers

The literature review identified cyber attacks on CNI resulting in a loss of access to goods and services among consumers. The specific impacts of this will depend on the CNI impacted. For example, the Wannacry incident on the NHS resulted in an outage of the EMIS Health system[50] which prevented many GPs from being able to digitally manage appointment bookings, patient records and prescriptions; and delayed urgent tasks and referrals.[51] The literature also finds that prolonged loss of service can also affect consumers' confidence and trust.[52]

Further, cyber incidents can result in an increase in the price of goods or services if they reduce the available supply of goods and services such that excess demand puts pressure on prices. For example the ransomware attack on the Colonial Pipeline in 2021 was found to have led to an average fuel price increase of 4 cents per gallon.[53] Such price increases can have a negative impact on the disposable income of consumers and reduce consumer surplus.[54] Consumer surplus is the difference between the maximum price a consumer would be willing to pay for a good or service and the actual price paid by the consumer[55] and therefore represents the net benefit they receive from a transaction. If prices rise, the consumer's surplus decreases all else being equal. If a consumer is prevented from undertaking a purchase their loss is equal to the consumer surplus of the foregone transaction.

Studies looking specifically at the potential impact of cyber incidents on rail networks identified the following outcomes and impacts for consumers. It is noted that these identified impacts are from studies looking at hypothetical events or from other countries or circumstances so may not directly apply to the scenario considered in the study:[56, 57]

— Reduced service levels across the affected parts of the network, leading to a reduction in passenger journeys and/or longer journey times for passengers. Where passengers experience longer journey times or they are unable to travel to leisure activities there may be a loss of welfare.

— Loss or delay of goods transported using the freight rail may result in shortages of products.

[47] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[48] Ibid.
[49] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493.
[50] The EMIS Health system supplies electronic patient record systems and software used in the NHS.
[51] Ghafur et al (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digit. Med.* 2, 98 (2019).
[52] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[53] T. Tsvetanov, S. Slaria. (2021) The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters Volume 209, December 2021, 110122
[54] Ibid.
[55] Marshall, A. (1920) 'Appendix K: Certain Kinds of Surplus', in Principles of Economics (8th ed.). London: Macmillan and Co. Ltd. Available at: https://www.econlib.org/library/Marshall/marP.html?chapter_num=67#book-reader
[56] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science
[57] Reitšpís, J., & Mašľan, M. (2021). Possibilities of prevention and reduction of threats affecting the safety and fluidity of land transport. Baltic Journal of Economic Studies, 7(4), 18-23.

— Potential loss of life if an attack results in the unsafe movement of trains.

— Loss of public confidence in railway operators.

Impacts to the wider economy

To the extent that a cyber incident impacts businesses and consumers, this can feed through into wider impacts on a country's economy. By definition, such wider impacts are an expected feature of systemic cyber incidents. The literature identifies that one of the key economic impacts of cyber incidents is a loss of productivity and output as business operations, for both the business affected and those in the downstream supply chain, are disrupted, with a subsequent impact on a country's Gross Domestic Product (GDP).[58]

The complexity of the supply chains in which CNI are embedded can lead to cascading effects on other sectors of the economy.[59, 60] Further, the global nature of present-day supply chains means that the impacts of cyber attacks may not be contained to the country targeted but may have international implications.[61]

The scale of the impact of a cyber incident to CNI can also be driven by the market concentration of the sector. When there is a higher concentration of firms owning and operating CNI, a cyber incident could have a greater impact on the economy as many more firms in the downstream supply chain will be connected.[62] This is relevant when considering CNI where there are natural monopolies present such as in the rail and energy sectors.

2.2.3 Estimated economic costs of a systemic cyber incident on the rail network

Research question 3: What are the economic costs of the attack?

There is limited evidence from existing literature on the potential economic costs of a systemic cyber incident on the rail network. It is noted in studies that it is difficult to estimate the economic costs of a cyber incident to the rail network as there is insufficient public information on the extent to which a cyber incident might disrupt the operations of rail services.[63]

However, evidence from cyber incidents on other forms of CNI provide useful insight on how cyber disruptions can have economic effects in terms of inoperability and damage to specific sectors of the economy, which in turn impact GDP.

A 2016 study by Kelly et al[64] estimated that a power blackout in the UK due to a cyber incident lasting between 3 and 12 weeks would produce economic losses to individual sectors in the range of £11.6 billion to £85.5 billion (£16.0 billion to £117.6 billion in 2024 prices).[65] Financial services; wholesale and retail trade; real estate activities and professional services sectors were expected to experience the greatest losses. The expected overall long-run impact of the attack on GDP was estimated to amount to a loss of between £49 billion to £442 billion (£67 billion to £608 billion in 2024 prices) [66]

[58] Eling, M., Elvedi, M., & Falco, G. (2022) The Economic Impact of Extreme Cyber Risk Scenarios. North American Actuarial Journal, 27(3), 429–443.
[59] Ibid.
[60] Tam et al (2023) Quantifying the econometric loss of a cyber-physical attack on a seaport. Front. Comput. Sci., 23 January 2023 Sec. Computer Security Volume 4 - 2022
[61] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[62] KOVRR (2024) The UK Cost of the CrowdStrike Incident.
[63] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science
[64] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[65] Figures updated to 2024 prices using the GDP deflator. Source: HMT (2024) GDP deflators at market prices, and money GDP October 2024 (Autumn Budget 2024) - GOV.UK
[66] Figures updated to 2024 prices using the GDP deflator.

across the entire UK economy in the five years following the outage when compared against baseline estimates for economic growth.

Another study modelling the impact of a 5-day cyber disruption on the electricity distribution network serving the London area estimates GDP loss ranging from £20.6 million up to £111.4 million (£25.7 million to £139.0 million in 2024 prices).[67] [68]

Besides GDP impacts, studies have analysed the potential cost to the economy through other metrics:

- Oughton et al. measure lost investment the UK economy ranging from £6 million to £34 million (£7 million to £42 million in 2024 prices) in the scenario of a cyber-physical attack disrupting the electricity network in London, while lost capital stock formation is estimated to range from £12 million to £74 million (£15 million to £92 million in 2024 prices).[69] [70]

- Some studies include loss of life as a potential consequence of cyber-physical attacks to critical sectors of the economy. For instance, it is estimated that an attack to the rail network causing "unsafe movement" of a convoy could cause an accident with 100 or more deaths in the worst-case scenario.[71]

2.2.4 Methodologies used to model the economic costs of systemic cyber incidents

Research question: What is the best methodology to model such an attack?

The literature review identified a number of commonly used methods to model the economic costs of systemic cyber incidents which are summarised below. Each has its pros and cons, with the 'best' methodology depending on the objectives and parameters for the analysis:

- Most studies are based on economic modelling and other related econometric analyses. Studies often rely on inoperability Input-Output models, that is computer-based models that analyse the impacts created by disruptions on the interactive operations of economic and infrastructure sectors.[72, 73] These have the benefit of being replicable, generalisable and scalable, but lack the specificity of bespoke analysis based on behavioural response and wider context, and typically omit broader, difficult to quantify, impacts.
- To account for qualitative factors of a specific scenario, some studies triangulate quantitative modelling with structured interviews with stakeholders and representatives of critical industries, government, and regulatory agencies[74]. These have the benefit of being able to take into account specific impacts based on the context of the attack and capturing harder to quantify impacts. However, they are more resource intensive to implement due to the requirement for primary research (e.g. interviews with a large range of informed stakeholders).
- Where data allows, studies often deploy system-dynamics models or sectoral analyses to simulate how consumers are affected by disruptions like price hikes, internet shutdowns, and

[67] Figures updated to 2024 prices using the GDP deflator.
[68] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[69] Figures updated to 2024 prices using the GDP deflator.
[70] Ibid.
[71] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. International Conference on Reliability, Safety and Security of Railway Systems.
[72] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[73] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[74] Ibid.

transport failure as a result of attacks on CNI.[75, 76, 77, 78] These have the benefit of offering the most comprehensive and insightful modelling, providing a much richer picture of the integrated financial and non-fungible costs of an attack. However, the requisite data is very difficult and expensive to acquire and the analysis takes time. Furthermore, these types of studies tend to be very bespoke, which can limit their generalisability.

Due to the inherent difficulties in gathering data about cyber disruptions to critical infrastructures, the majority of studies are not primarily based on real-world data. One example of an exception to this is a retrospective analysis of the impact of the Wannacry attack on the NHS, which uses data from Hospital Episodes Statistics to determine the number of cancelled outpatient appointments, the impact on emergency and elective admissions, the number of accident and emergency (A&E) attendances, deaths, and the financial impact on activity.

[75] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493.
[76] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[77] T. Tsvetanov, S. Slaria. (2021) The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters Volume 209, December 2021, 110122
[78] Petermann et al (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage.

3 Mapping of the economic cost of a cyber incident to the rail network

In considering the specific scenario of a systemic cyber incident on the rail network, impact mapping was used to understand the routes through which economic costs may be realised and any dependencies or specific conditions that may be relevant to these. The impact map is used to detail the potential outcomes and impacts that may arise as a result of a systemic cyber incident to the rail network. It shows the causal link between stages of the theory of change and helps support the attribution to the end impact on the UK economy, at least in part, back to the initial shock of the systemic cyber incident. Figure 3.1 below presents the impact map of the cyber incident to the rail network under the given scenario.

The impact map was developed following engagement with stakeholders from DSIT, DfT and Network Rail to better understand the parameters of the scenario and how different economic agents may respond. In addition, the impact map reflects insights and findings from the literature review on the types of impacts that may be realised, or would be expected to be realised, following a cyber incident on the rail network.

The impact map shows the potential impacts split across the main areas of impact detail within Section 1.3.1, including direct financial impacts to the organisation that is subject to the attack; indirect impacts to passengers/consumers and businesses; and wider economic impacts realised across the economy.

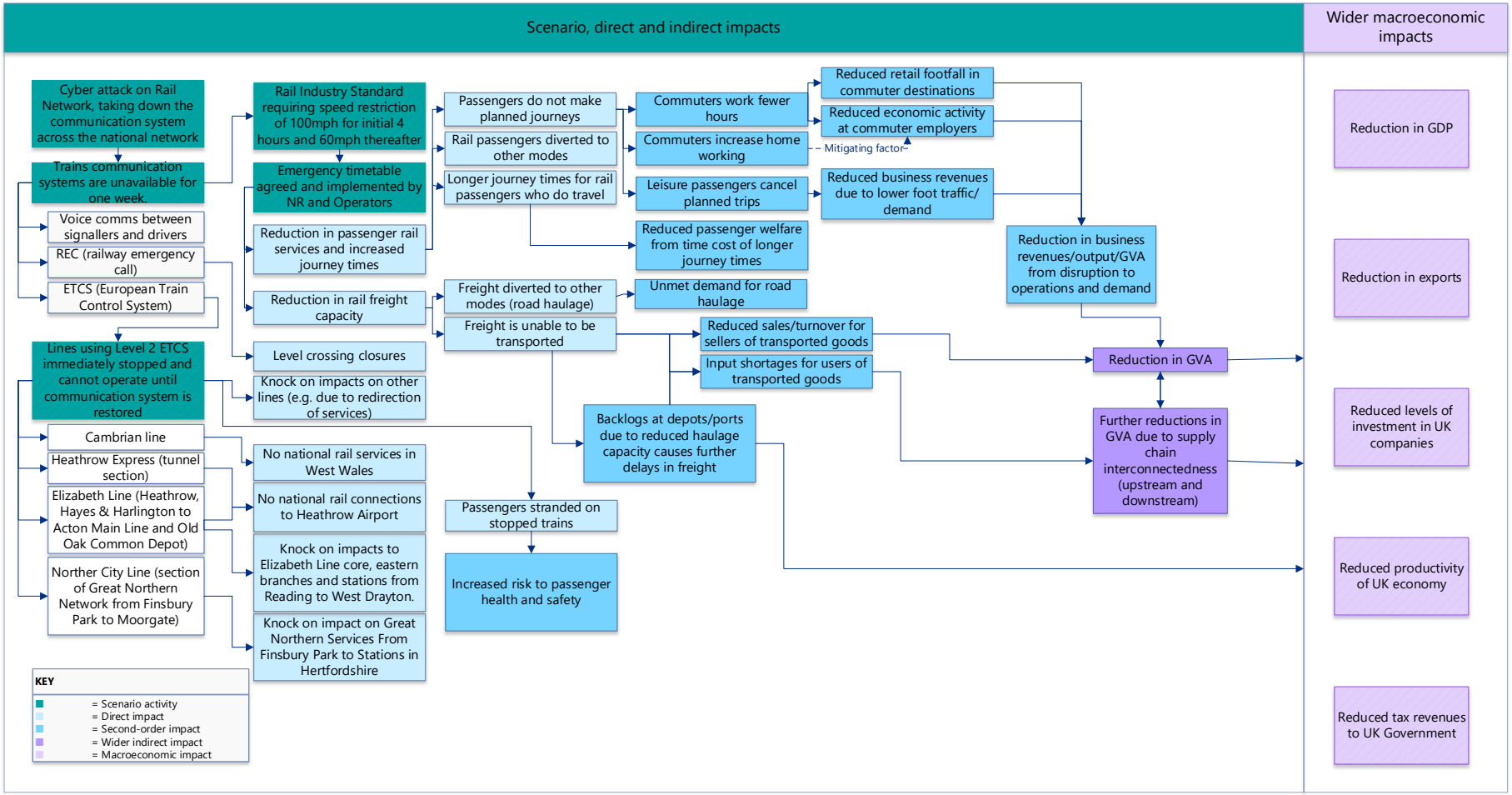
The categories of economic impact are analysed in turn in Sections 4 and 5.

Based on prioritisation of these impacts alongside DfT and DSIT (as detailed in Section 1.3.4), the following impacts were included for quantification in the modelling:

- Direct financial cost to the targeted organisation
- Economic costs to train and freight operators
- Economic and welfare costs to passengers as a result in train delays and cancellations
- Economic costs to business of lost productivity due to lost workdays
- Economic costs to business of supply chain disruption
- Wider economic impacts through the UK supply chain

Other impacts identified, but not prioritised for quantification, are assessed qualitatively based on available data, literature and consultation with DfT and Network Rail.

Figure 3.1: Impact map of a systemic cyber incident to the rail network under the given scenario



Source: KPMG analysis

4 Direct financial cost of a systemic cyber incident to the GB rail network

4.1 Introduction to the section

This section sets out findings in relation to the direct financial costs to the organisation that is subject to the cyber attack. In the scenario under consideration, based on consultation with DfT it is assumed that Network Rail is the targeted organisation. For the purposes of this study, analysis is focused on the direct financial impact on the organisation should the threat scenario occur.

The direct financial impacts to Network Rail included in the analysis comprise costs such as productivity costs of operational disruption, incident response, recovery, fines or regulatory costs, as a result of the cyber attack materialising.

4.2 Approach to the assessment of direct financial costs

As part of the development of the hypothetical systemic cyber incident scenario, consideration was given to the nature of a cyber attack that would result in a systemic impact on national rail services. KPMG's view is that, for a cyber attack to result in the scale of impact described in the scenario it would most likely need to be an attack impacting operational technology (OT). For the purposes of the assessment of direct financial costs, this is assumed to be a widespread ransomware attack.

For a given attack type, the financial impact can vary based on the specific nature of the attack. When modelling cyber risk, risk exposure is typically expressed in a financial range to demonstrate the potential loss should the scenario occur, across most likely and worst-case (high impact, low likelihood) scenarios.[79] The potential costs can vary considerably depending on the scenario. For example, based on KPMG's Cyber Risk Insights[80] industry insights database, for an organisation in the transportation industry with a revenue band between £8 billion and 79 billion, you could expect £800k direct financial loss from a widespread ransomware scenario is a most likely scenario however, in the worst case, potentially suffer a loss of up to £177 million.

For the purposes of this study, bespoke analysis had been undertaken to identify the likely 'reasonable worst case' direct financial costs of a widespread ransomware attack based on the parameters of the scenario. The approach utilised to assess the direct financial impact of this scenario aligns with Open FAIR™ risk analysis.[81]

FAIR™ refers to impact as 'loss magnitude' and typically breaks it down into the following groups:

- Productivity: Loss resulting from the inability to deliver core services or products
- Response: The costs of managing the incident response
- Replacement: Loss resulting from replacing or rebuilding assets such as hardware or data
- Competitive Advantage: Loss resulting from damage to an organisation's competitive differentiators such as intellectual property

[79] The most likely value represents the most probable or expected outcome. The worst case is often calculated to a 95% confidence level, meaning the estimation is that there's a 95% chance that the actual cost will be lower than this figure. Taking the 95% value helps protect against extreme outliers or unforeseen issues.
[80] KPMG Cyber Risk Insights (CRI) is a cyber risk quantification SaaS solution that takes a threat-led approach to measuring cyber risk. The industry insights database contains approximately 1,500 individual datapoints. The loss event examples in the databases come from several sources, including Cyentia's IRIS report, various threat reports and data from KPMG's internal Cyber Response Services team. The data maps are mapped to five revenue bands, 20 industries, and the 12 pre-modelled threat scenarios in CRI.
[81] Open FAIR™ risk analysis is a risk management framework for breaking down the factors that contribute to risk and how they affect each other. It provides a taxonomy for deconstructing the likelihood and impact from loss events.

- Fines and Judgements: Legal, regulatory or contractual costs
- Reputation: Financial loss as a result of negative perception on the organisation from external stakeholders, such as contracts with third parties, or a loss of customers

The breakdown of estimated values against each of these aspects, along with details of how each value was derived, is provided below (Section 4.3).

Longer term competitiveness and reputational impacts on the organisation of the systemic cyber incident have not been included in the financial impact analysis. As a natural monopoly, such impacts on Network Rail would likely be limited.

4.3 Estimated direct financial costs

The estimated direct financial impact to Network Rail resulting from the cyber incident scenario is **£123.0 million** in 2024 prices. It is noted that this cost would vary based on several factors and therefore is indicative only.

The breakdown of estimated costs is detailed below.

Table 3: Estimated direct impact from the widespread ransomware threat scenario

Cost area	Description	Assumptions	Direct impact
Productivity	Productivity is the loss resulting from an operational inability to produce/deliver products and/or services. The productivity cost is the financial impact of not being able to operate trains during the period of disruption. Gross profit is a useful metric for estimating productivity loss because it directly reflects the impact on revenue generation and operational efficiency.	Assessment utilises Network Rail's 2024 profit before tax of £1.5 billion[82] and the days of operation (365 days per year). The estimated number of days of business interruption is 7 days.	£9,512,000
Incident Response	Incident response is the loss resulting from the immediate cost of managing the event (i.e. digital forensics and incident response).	The hours and costs of incident response were estimated based on averages from previous assessments made by KPMG using CRI. It has been assumed that there are 140 hours available on an incident response retainer and any hours above this are at additional cost. It is estimated the response takes 7 days of response, with 20 people working on the response (1,120, and 980 when using the remaining retainer hours), at an assumed rate of £350 per hour. This brings the incident response cost to approximately £343,000. In light of draft government policy to reduce ransomware payouts by CNI, this scenario assumes no ransom is paid. Potential ransom costs are therefore not included.	£343,000
Recovery	Recovery includes losses incurred because of the time spent having to restore system(s) or service(s) to their normal state (i.e. incident recovery). It also includes losses incurred as a result of having to replace capital assets impacted	In the absence of more specific assumptions on incident recovery costs, a ratio of incident recovery costs to incident response costs (in terms of time/effort) of 2:1 has been applied based on insight in relation to typical ratios seen by KPMG's Cyber Incident Response team in relation to widespread ransomware incident. This is an indicative ratio based on	£784,000

[82] Network Rail 2024 annual report, financial statements

	by the incident (i.e. replacement loss).	the experience of the KPMG team across a range of types and scales of incidents across sectors. As the incident response retainer hours would have used, it is assumed there are none left to cover recovery. Any asset remediation or rebuild costs have not been included for the purposes of this study, but would add to the recovery costs.	
Fines & Judgements	Legal and regulatory losses are those resulting from not complying with relevant laws and regulations.	Network Rail could be susceptible to fines under cyber security legislation. Network Rail stakeholders suggest that the *trains communications system* is in compliance and fully managed. However, if Network Rail failed to report or respond appropriately to the attack, it could still be subject to a financial penalty. The logic for a worst-case GDPR fine has been utilised as a proxy. The 'standard maximum amount' is used assuming that the information is not special category PII, and a multiplier is applied to account for the seriousness of the incident and degree of culpability.[83]This results in an estimated fine of £2.9 million. This level of fine can be compared with other recent worst-case penalties from cyber incidents, such as the ICO penalty issued to Advanced Computer Software Group Ltd of £3.1 million for the 2022 ransomware attack impacting the NHS.[84] If the ransomware incident also included a data breach off the back of the ransomware incident the fines would be higher. However, the scenario utilised for this research is an availability disruption only so additional fines are not included. In addition to a financial penalty from a regulator, Network Rail's track access contracts[85] with train and freight operators include Network Rail's performance regime – a legal requirement to compensate train and freight operators for losses that arise from delay and cancellations they cannot control. Network Rail estimates that payments of approximately £109.5 million would be expected in the cyber attack scenario.[86]	£112,400,000

Source: KPMG analysis based on data from Network Rail and KPMG's IID

[83] It is assumed that the level of serious is low because Network Rail have the relevant safeguards in place to protect data. It is assumed they would notify the regulator in the situation of a breach but might not have completed all expected actions within a timely manner (such as notifying organisations). Therefore we have taken Network Rail's revenue of £11.5 billion and applied a 0.25% multiplier to account for negligence, a 50% penalty reduction for reporting the breach in a timely manner, and a further 20% reduction for being in a position to pay the penalty within a timely manner. The calculation logic is based on the ICO Statutory guidance on enforcement action.

[84] Software provider fined £3m following 2022 ransomware attack. See: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/

[85] See: track-access-model-passenger-contract.docx

[86] This assumes an estimated daily payout in the case of a total network shutdown of £25.6 million based on previous strike data. Using data from Storm Eunice as a proxy, in the scenario it is assumed the number of trains reduces by 61% resulting in an estimated a cost in the case of the cyber attack scenario of £15.6 million per day (61% of £25.6 million).

5 Economic impact of a systemic cyber incident to the rail network on wider stakeholders

5.1 Introduction to the section

This section sets out findings in relation to the indirect impacts and wider economic impacts of a systemic cyber incident to stakeholders beyond the organisation that is subject to the attack (Network Rail). It includes impacts on train and freight operators, passengers/consumers, other businesses and the wider economy.

Assessment of these impacts was carried out using a combination of quantitative economic modelling and qualitative assessment. Where impacts are included as part of the quantitative modelling, a summary of the approach taken is included in the relevant sections below, alongside key findings of the analysis.

5.2 Economic impacts on train and freight operators

Under the scenario (detailed in Section 1.2), it is assumed the cyber attack on the rail network has an impact on the operation of rail services across GB. Specifically, any rail services utilising Level 2 ETCS will immediately stop operating following the cyber incident and will not be able to operate until the system is recovered, which will take one week. As of February 2025, rail lines utilising Level 2 ETCS include:

- Cambrian line
- Thameslink Core (London Blackfriars to St Pancras International)
- Elizabeth line (Western section Heathrow to Great Western Mainline)
- Northern City Line (Moorgate to Finsbury Park)

In addition to the cessation of Level 2 ETCS services, there would be higher levels of cancellations across other lines. Specifically, four hours after the *trains communications system* service being down, rail speeds must be reduced to 60mph until the *trains communications system* service is restored (assumed to take a week). The slower running of trains across the network would likely result in services being cancelled, as fewer trains are able to move across the network.

As noted in Section 1.3.5, data from Storm Eunice, which resulted in multiple line closures and national speed limits being reduced to 50mph across the national rail network, is used as a useful proxy for the potential impact of the cyber incident scenario on the rail network. Based on data relating to Storm Eunice, provided by Network Rail, it is assumed that the cyber incident on the rail network would result in a 19% reduction in the number of scheduled trains and a further 42% of scheduled trains being cancelled on the day. Overall, this would result in 53% of scheduled trains being cancelled and, based on data from Network Rail, there would be an assumed 61% reduction in the total distance (as measured in kilometres) run across the rail network per day. This would affect both passenger and freight trains, with the same proportionate impact assumed across both.

This reduction in the number of trains that are able to operate would generate a loss of revenue to train operators and freight operators.

In relation to train operators, data from Network Rail suggests that the reduction in trains operating would result in a fall in the number of passenger journeys of approximately one third, with a corresponding fall in train operators' revenues over the period of disruption. Train operator revenues are estimated based on the revenue of the 'passenger rail transport, interurban' sector for 2022 from the Annual Business Survey (ABS)[87]. Based on this, a revenue impact of £11.7 million (in 2024 prices) per day is estimated, equating to a revenue impact of £81.9 million over the course of the week. This equates to a GVA impact of £37.5 million.[88] In addition to the direct revenue impact there would be increased costs of compensation payouts to passengers.

For freight, given less flexibility in capacity compared to passenger rail, the impact on freight moved (in million tonne kilometres) would be expected to fall more proportionately in line with the reduction in distance run. A 61% reduction in revenues per day over the period of disruption is therefore assumed based on the assumed reduction in total distance travelled across the network as a result of the attack. Freight operator revenues are estimated based on the revenues for the 'rail freight transport' sector for 2022 from the ABS. Based on this, a revenue impact of £2.2 million per day is estimated, equating to an impact of £15.7 million over the course of the week of disruption. This equates to a GVA impact of £5.7 million.[89]

However, as noted in Section 4, Network Rail's track access contracts with train and freight operators[90] include regimes through which train and freight operators are compensated by Network Rail for planned and unplanned service disruption. On this basis, it is assumed that the direct impact on train operators and freight operators is neutral and costs are borne by Network Rail. Therefore, they are captured within the assessment of direct financial impacts, as reported within Section 4.

The indirect impact through operators' supply chains is considered within the wider economic impacts within Section 5.5.

5.3 Economic impacts on passengers/consumers

5.3.1 Impact on passengers of forgone journeys

The data relating to Storm Eunice, reported in Section 5.2 provides an indication of the impact of the cyber attack on passenger rail services.

In terms of the impact on travel, Network Rail provided estimates that during Storm Eunice, passenger numbers fell by approximately one-third. It has been assumed that a similar drop in passenger numbers would result from the cyber incident.

Those who can no longer travel by rail due to the disruption to the operation of rail services, would need to choose a different mode of travel (including public or private transport) or not undertake the journey at all. Evidence from DfT on the impact on passengers of the rail strikes over the summer and early autumn of 2022[91] provides an indication of how rail passengers may respond to the disruption of rail services from the cyber incident.[92] The strike survey indicates that of those that that were unable to make their journey by train, approximately two thirds did not travel, whilst approximately one third travelled by alternative modes of transport.[93]

[87] ONS, 2022. Non-financial business economy, UK (Annual Business Survey): - GOV.UK
[88] ONS, 2022. Non-financial business economy, UK (Annual Business Survey): - GOV.UK
[89] ONS, 2022. Non-financial business economy, UK (Annual Business Survey): - GOV.UK
[90] See: track-access-model-passenger-contract.docx
[91] DfT (2023) Rail strikes: Understanding the impact on passengers – full report
[92] It is, however, noted that the strikes in question occurred on only 2-3 non-consecutive days in any given week and therefore would allow for greater mitigation of impacts among those affected (e.g. changing day of travel) than would be possible in the cyber incident scenario.
[93] Due to respondents being able to select multiple responses in relation to what they did instead of travelling by rail on the day(s) they were planning to, and the wording of survey response options, precise estimates of the proportion that still made their journey cannot be obtained.

For those who are unable to, or choose not to, travel, impacts would be expected as a result of not being able to attend work, education or undertake leisure/social activities, as follows:

- Travelling for work: Data from DfT shows that in 2023, 10% of the population of Great Britain used rail (including National Rail, underground, light rail and tram) to travel to work.[94] Among these, those that travel by National Rail services affected by the cyber attack may struggle to continue to travel to work for the period of disruption. To the extent that people are unable to work as a result of the disruption (e.g. due to not being able to travel by other means or work from home), this could have an impact both in terms of their personal finances, through potential lost wages, and on the economy in terms of lost economic output as well as impacts on public services.

  The rail strike survey provides some insight into the extent to which people may be prevented from travelling to work as a result of the rail disruption. Commuters made up the largest share of survey respondents who had planned rail travel during the strike week – at 57% of all those who had planned journeys. Among these 30% did not travel and worked from home instead; 13% reported working less; whilst 6% stated that they were not able to work at all.[95] In terms of personal impact of this work disruption, 31% of those who had planned to commute to/from work reported a financial loss due to strike action, with 16% reporting a personal loss of earnings. The quantified impact on earnings as a result of people being unable to travel to work is included within the productivity impact assessed in Section 5.4.1.

- Travelling to and from education: Passengers who use rail services to travel to and from education may be prevented from accessing school, college or university if alternative travel arrangements cannot be made. There may in turn be a welfare impact on those who are not able to access education for the duration of the disruption. However, the impact of this is likely to be relatively small. Data from the National Travel Survey shows that in England, only 1% of trips to education and/or to escort others to education are taken by rail[96] and data from the strike survey identified that among those that planned to travel by rail for education, only 18% had to study less than planned and 7% were unable to study at all. For the few affected, evidence suggests there could be some, though limited, impact on educational outcomes and future earning potential.[97]

- Travelling for leisure and social purposes: As of 2022-23, approximately 58% of all rail trips were undertaken for leisure purposes.[98] The positive relationship between leisure engagement and both physical and mental health has been evidenced in many academic studies[99] which identify a wellbeing benefit of leisure and social activities. To the extent that the cyber incident to the rail network prevents people from being able to undertake leisure and social activities, this would represent a welfare cost to these individuals who are unable to travel. The strike survey provides an indication of the impact of rail disruption on leisure activities, finding that among those who planned to travel by rail for leisure, only 44% made the journey, 23% spent less time with family as a result, and 41% had to rearrange social plans.

It is noted that whilst those unable to travel may face financial or welfare costs, as described above, they may also experience a financial benefit by saving on travel and other related costs e.g. purchasing food and drink whilst travelling.

[94] DfT (2024) Transport Statistics Great Britain: 2023 Domestic Travel
[95] DfT (2023) Rail strikes: Understanding the impact on passengers – full report. Note, respondents could select multiple response.
[96] DfT (2024) National Travel Survey
[97] DfE (2016) The link between absence and attainment at KS2 and KS4. Note this study relates to the impact of a day of school closure, and therefore cannot be directly used to assess the impact of individual absence, though
[98] GBRTT (2023) Rest and recreation tops reasons for train trips – new analysis
[99] Fancourt et al (2021) How leisure activities affect health: a narrative review and multi-level theoretical framework of mechanisms of action. Lancet Psychiatry. 2021 Feb 11;8(4):329–339.

5.3.2 Impact on passengers of longer journey times

As set out in the scenario detailed in Section 1.2, it is understood that as a result of the cyber incident on the rail network, after four hours rail speeds must be reduced to 60mph until the trains communications system service is restored. This reduction in the maximum speed that the rail network can operate at would result in longer journey times for passengers. Similarly, journey times may be impacted by amended service timetables discussed above, as services prioritise running services that stop at all stations as opposed to fast services.

For passengers that continue to travel, longer journey times represent a time value cost. This is time that passengers could have otherwise utilised for work, contributing productively to the economy; or for leisure, providing them with a welfare benefit e.g. socialising or engaging in culture.

Delays to passengers' journeys will be generated through two routes. Firstly, based on the experience of Storm Eunice, it is expected that for scheduled trains that continue to run, services will experience additional delays compared to average service. Secondly, on-the-day cancellations will create additional wait time at stations for those intending to travel on cancelled trains. The costs of these delays are considered below.

Data provided by Network Rail on the level of disruption from Storm Eunice in 2022 has been used as a proxy for the impact on journey times. This suggests an average train delay of 8.6 minutes, compared to an average of 1.3 minutes on a normal day, representing an increase of 7.3 minutes from average. The time cost for purposes of work is typically measured using average wage data as a proxy for the value of time that could otherwise be spent at work.[100] Data from the DfT Transport Appraisal Guidance (TAG) provides data on the value of working time for a rail passenger, as well as non-working time for commuting and leisure trips. It has been assumed that the value of time for business travel passengers is £38.84 per hour; for commuting passengers it is £13.25 per hour and for leisure passengers it is £6.05 per hour.[101,102]

Based on the assumption that passenger numbers would reduce by one-third as a result of the cyber incident, it is estimated that 20.6 million passenger journeys would be undertaken over the course of the week.[103] The number of passengers, split by journey purpose, was estimated using data on reason for travel from GBRTT.[104] Applying the net average increase in train delays of 7.3 minutes and the value of time, split by journey purpose, from the DfT TAG, it is estimated that the value of rail journey delays associated with the cyber incident would be £26.9 million.

To estimate the delays caused by cancelled trains, the ORR's Cancellation Minutes Multiplier (CMM) of 90 mins[105] is used. The CMM has been applied to the estimated number of passengers whose journeys would be cancelled. This is estimated based on the average passenger journeys per week sourced from the ORR[106], the estimated proportion of trains that are cancelled (based on Network Rail data from Storm Eunice) and the value of time split by journey purpose from the DfT TAG. Based on this approach, it is estimated the value of cancellation delays would be £254.5 million.

Combining the value of rail journey delays and the value of cancellation delays, it is estimated that overall the cyber incident would result in £281.3 million in value of lost time for passengers.

[100] Department for Transport (2024) TAG data book
[101] Value differs between the factor cost, perceived cost and the market price.
[102] All figures are in 2024 prices.
[103] Based on an average of 30.8 million passenger journeys per week for the period April 2023 to March 2024. Sourced from: ORR (2024) Table 1220 – Passenger journeys
[104] GBRTT (2023) Rest and recreation tops reasons for train trips – new analysis
[105] ORR (2023) PR23 recalibration of the Network Rail passenger Schedule 8 regime: methodology report dated 22 November 2023
[106] Based on an average of 30.8 million passenger journeys per week for the period April 2023 to March 2024. Sourced from: ORR (2024) Table 1220 – Passenger journeys

5.3.3 Impact on wider consumers

As noted in Section 5.3.2, whilst some of those unable to travel by rail may not travel at all, around two thirds would be expected to travel by alternative modes of transport.[107] This may create additional costs for those travelling. For example, evidence from the rail strike survey showed that amongst those that had planned to travel by rail, 14% reported increased travel costs.[108]

Diversion to alternative modes of transport could also put greater pressure on other transport networks, particularly given that within the scenario it is assumed that there would be limited ability for additional public transport to be run to mitigate the impact of the rail disruption. Results from the strike survey provides an indication of where greatest pressure may be felt. Specifically, of those surveyed who were unable to make a planned rail journey due to the rail strikes:

- 17% travelled by car/motorbike/van
- 11% travelled by bus/coach
- 6% travelled by tax/minicab
- 5% travelled by another form of public transport
- 3% cycled or walked

The emphasis on mode-switch to private transport (car/motorbike/van) suggests the greatest impact may be on levels of congestion on the roads, leading to potentially longer journey times for all road users, not just those who are switching from rail to road, and increased CO_2 emissions. In addition, mode shift to other forms of public transport means that, alongside increased crowding on those rail services that continue to operate, other public transport systems would be expected to see higher levels of demand and result in a crowding of service, particularly in peak periods. Quantification of the impacts of mode-shift (e.g. on emissions and journey times) would rely on further information on how modal shift varied by journey length which is not known. These impacts have, therefore, not been quantified in the analysis.

5.3.4 Impact on passenger safety

The cyber incident on the rail network may also negatively impact passenger safety, resulting in welfare costs for passengers. There are several routes through which this impact may occur:

- Stranded passengers: As noted in the scenario, the cyber incident would cause rail lines utilising Level 2 ETCS to immediately cease operating. Passengers on those rail lines at time of the cyber incident would be stranded. While there are procedures in place which are enacted successfully on a regular basis to deal with such events[109], a larger than typical number of stranded passengers could pose an additional risk to passenger health, safety and security. For example, in 2018, following being stranded due to a large storm, passengers in Lewisham self-detrained onto tracks that were still open to traffic and where the third rail was live.[110] This not only put the passengers at risk but also caused disruption to other trains operating on the line.
- Crowded stations, platforms and trains: The cyber incident on the rail network is expected to result in fewer rail services being run and higher levels of train cancellations. Lower

[107] Due to respondents being able to select multiple responses in relation to what they did instead of travelling by rail on the day(s) they were planning to, and the wording of survey response options, precise estimates of the proportion that still made their journey cannot be obtained.
[108] DfT (2023) Rail strikes: Understanding the impact on passengers – full report
[109] Network Rail & Rail Delivery Group (2020) RDG and Network Rail Guidance Note: Meeting the Needs of Passengers Stranded on Trains
[110] GOV.UK (2019) Report 02/2019: Self-detrainment of passengers onto lines that were still open to traffic and electrically live at Lewisham

throughput of trains through stations may mean that passengers flows are not as well distributed, leading to crowding at stations, platforms and on trains. The ORR states that there is not clear evidence for increased health and safety risks to passengers from crowding.[111] However, it is also noted by the ORR that some passengers report slips, trips and falls at crowded stations and on crowded trains. Further crowding may increase the risk of passengers fainting, particularly in instances of hot weather. Similarly, there is evidence of crowding scenarios increasing feeling of stress, anxiety and vulnerability – impacting the wellbeing of passengers.[112]

It is unclear the extent to which the cyber incident on the rail network may impact passenger safety as there is limited evidence on which to draw. It is, however, noted that there are mitigations that can be put in place by train operators, Network Rail and other parties involved in the management and operation of the rail network. These mitigations would go some way to manage and lower any potential increased risk to passenger safety.

5.3.5 Distribution of passenger impacts

In terms of the distribution of impacts, the impact of disruption to rail services due to a cyber incident on the rail network may not be equally distributed across the UK. Data from the Office of Rail and Road (ORR) shows that between April 2023 and March 2024, London and the South-East had the highest number of passenger rail journeys to, from and within the region.[113] Therefore, it could be considered that these regions could experience higher levels of impact, reflecting the greater usage of and reliance on rail travel in these regions.

5.4 Economic impact on business

5.4.1 Impact of lost work days

As set out in Section 5.3.1, among those who planned to travel for work during the period of the cyber attack, some would not be able to work at all as a result of travel disruption. This would result in a loss of output for the duration of the time that they are unable to work. This could result in a loss of earnings for individuals and a loss of revenue and associated profit for business.

The potential impact of lost work days as a result of the rail disruption has been valued in terms of the lost GVA[114], reflecting both lost earnings and lost business profit.

Evidence from the rail strike survey indicates that 4% of all those that had planned to travel on a strike day were unable to work at all as a result of the strike.[115] For the purposes of the analysis, to estimate the total number of lost work days the findings of the strike survey have been applied to the estimated number of business and commuter passengers who would no longer travel by rail as a result of the cyber incident. It is therefore estimated that approximately 397,600 work days would be lost over the one week of disruption caused by the cyber incident.

To value the cost of lost work days, the average GVA per hour worked across all workers in the UK of £46.16 in 2023 (in 2024 prices) was sourced from the ONS.[116] Based on data from the ONS on working hours, it was assumed that, on average, people work 6.4 hours per day.[117] Applying this assumption to the average GVA per hour, results in an estimate of £293.57 (in 2024 prices) of

[111] ORR (2024) ORR's health and safety crowding position statement
[112] Ibid.
[113] ORR (2024) Regional rail usage April 2023 to March 2024
[114] GVA is largely made up of personal income (compensation of employment) and business profits excluding depreciation (gross operating surplus).
[115] DfT (2023) Rail strikes: Understanding the impact on passengers – full report. Note, respondents could select multiple responses. This equates to 6% of those who planned to travel for work.
[116] ONS (2025) Output per hour worked, UK
[117] ONS (2024) Average hours worked and economic growth, UK: 1998 to 2022

average GVA generated from a day of work. This figure was multiplied by the number of lost work days to estimate the total cost of lost work days.

Overall, it was estimated that the value of lost work days due to the cyber incident would be £116.7 million.

It is noted that there is no information on the industries in which those individuals unable to work due to rail disruption are employed. The GVA impact is estimated based on an average value of GVA per hour worked across the whole economy. However, if certain industries are more impacted by their workforce being unable to attend work due to rail disruption, the impact may be higher or lower, reflecting the relative value of output of workers in these industries.

5.4.2 Impact of reduced footfall/ consumer spending

Reduction in travel (particularly among those travelling for leisure purposes) would be expected to reduce retail, hospitality and leisure footfall and impact consumer spending during the period of disruption.[118]

Whilst this could have a temporary impact on business revenues, given the short nature of disruption, it is expected that some of this spending may be diverted e.g. to online retailers and/or local suppliers, or to a future date. This would limit the net impact of the disruption. This potential impact is evidenced in previous analysis by the ONS of the economic impact of strikes in the UK, including rail strikes.[119] Whilst the net economic impact may be limited, some businesses would likely experience loss of revenues, with convenience food and drink outlets, e.g. at stations, being most heavily impacted.[120] The time of year of the cyber incident would also affect the degree to which businesses are impacted, with any incident affecting seasonable periods (e.g. pre-Christmas) having a greater impact.

In terms of impacts associated with tourism, given the short term nature of the disruption, the impact on international tourists to the UK would likely be limited as travel plans would already have been made. However, domestic tourism and planned travel by international visitors within the UK may be impacted. These impacts would be captured within the impact on travel for leisure purposes discussed above.

5.4.3 Impact of supply chain disruption

As noted in section 5.2, alongside the impact on passenger rail, freight rail would also be impacted. Whilst freight operators would be compensated for losses resulting from the cyber attack, disruption to freight services will have a knock on impact through the supply chains they support.

The UK relies on inland freight transport to move goods around the country, including products, raw materials and finished goods. This transport enables businesses to meet their logistical needs and consumers to have access to the goods they need. DfT data[121] shows that as of 2022 rail freight made up 7% of freight moved[122] (measured in net tonne kilometres) and 4% of freight lifted[123] (measure in million tonnes), with a total of 74 million tonnes of freight carried by rail.

[118] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[119] ONS, 2023. The impact of strikes in the UK - Office for National Statistics
[120] ONS, 2023. The impact of strikes in the UK - Office for National Statistics
[121] DfT, 2024. Freight (TSGB04) - GOV.UK
[122] Freight moved measures the amount of freight moved on the railway network, taking into account the weight of the load and the distance carried. It is measured in net tonne kilometres.
[123] Freight lifted is the mass of goods carried on the rail network measured in tonnes, excluding the weight of the locomotives and wagons. Unlike freight moved it takes no account of the distance travelled.

Intermodal freight[124] made up the largest share of freight moved in 2024, accounting for 43% of freight moved. This was followed by construction products which made up 33% of freight moved.[125] Other key products carried include biomass (7%), metals (6%) and oil and petroleum (5%).

To mitigate the impact of disruption, it is expected that some rail freight would be diverted to road haulage. This is likely to be most feasible for intermodal freight. However, the extent to which it would be possible in practice depends on their being sufficient supply to meet the additional demand, which may not be the case given recent HGV driver shortages.[126] Any diversion of freight from rail to road would be expected to increase congestion and generate delays to both the delivery of diverted freight, and to other road users, including consumers and existing road freight.

In order to estimate the impact of supply chain disruption resulting from the cyber attack scenario, consideration has been given to the impact of delays to goods on subsequent production activity. This analysis focuses on the freight products accounting for the largest shares of freight moved.

Whilst intermodal freight makes up the largest share of all freight moved, its greater potential for modal shift to road is expected to mitigate the impact of delays to some degree. Furthermore, it is likely that some degree of catch-up growth following the disruption, or substitution between products, would be possible meaning that whilst there may be some impact on the range of goods available, the impact on output in the medium term likely would be limited. Given uncertainty as to the degree of potential mitigation of impacts and the lack of data on the specific products carried by intermodal freight, the potential supply chain impact resulting from disruption to intermodal freight has not been quantified.

Whilst it makes up a smaller (but still sizeable) share of rail freight moved, disruption to the delivery of construction products and industrial minerals[127] would be expected to have a greater economic impact due to the more limited potential for mode shift to road, and potentially less scope for substitution between products as construction inputs.

To estimate the impact of disruption to supplies of construction products as a result of the cyber attack, the value of construction products and industrial minerals moved per year is estimated. This is done based on these products' share of all freight moved[128] (36%), and an estimate of the total value of freight moved by rail per year of £30 billion[129] (in 2024 prices). This produces an estimated value of construction products and industrial minerals moved per year of £12.7 billion, or £243.3 million per week.

In the context of the cyber attack scenario, it is assumed that disruption to the rail network results in a reduction in freight moved during the week of the attack of 61% based on Network Rail data for Storm Eunice, equating to a reduction in the value of construction freight moved of £148.4 million during the week of disruption. This represents an estimated 17% of total intermediate consumption of construction products and industrial minerals[130] during the week of the attack, and 0.3% of annual intermediate consumption of these products.[131]

[124] This comprises products and raw materials transported in containers via multiple transport modes. Goods carried can include manufactured goods (including retail and intermediate goods), machinery and non-perishable food products.
[125] ORR, 2025 Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal
[126] UK government action to reduce the HGV driver shortage - GOV.UK
[127] These have been combined for the purposes of the analysis due to overlap within supply and use table product groups.
[128] ORR, 2025 Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal
[129] Based on an estimate relating to 2016 from a 2018 Rail Delivery Group report, 'Rail freight working for Britain', adjusted for changes in freight volumes since 2016 and uplifted to 2024 prices.
[130] These are assumed to include 'Other mining and quarrying, 'Manufacture of cement, lime, plaster and articles of concrete, cement and plaster' and 'Manufacture of glass, refractory, clay, porcelain, ceramic, stone products'.
[131] Sourced from ONS Supply and Use tables: ONS (2024) Input-Output analytical tables - Office for National Statistics

The sectors most reliant on these inputs are 'Other mining and quarrying', 'Manufacture of cement, lime, plaster and articles of concrete, cement and plaster', 'Manufacture of glass, refractory, clay, porcelain, ceramic, stone products' and 'Construction'. [132]

'Other mining and quarrying' is excluded from the analysis due to the relatively small size of the sector and due to the likelihood of secondary processes (e.g. crushing) to happen at the same site rather than materials being transported.

For the other key sectors affected, it is assumed that a 15% reduction would result in an equivalent fall in output during the period of disruption. This is on the basis of these products being key inputs to production for these sectors, however it is recognised that this represents an upper bound of potential impact and availability of this inputs may not fully constrain production. Based on this assumption, there would be an estimated reduction in GVA of these sectors of £520.1 million over the course of a week.

In relation to other key products carried by rail, biomass and oil and petroleum products are largely inputs to energy production. It would be expected there would be substitution to other forms of energy production in the event of reduced inputs from rail freight disruption in order to maintain supply. Given the small share of freight that other products make up, the impact of disruption to these has not been quantified.

In addition to domestic freight impacts, 89% of intermodal rail freight in 2024 was maritime intermodal[133], meaning that freight passes through UK ports for shipping. Disruption to the movement of these goods would be expected to have knock on impacts on ports, if onward movement of goods is affected, with potential subsequent impacts on international trade.

5.5 Wider economic impacts through the UK supply chain

The impact on train and freight operators, and wider businesses impacted through lost working days or supply chain disruptions will have a knock-on effect through the economy, through reducing demand throughout these businesses' supply chains. Reduced demand through the relevant supply chains would result in lower output, revenue and profit for supply chain businesses affected. A fall in economic activity at these businesses would reduce the level of value added to the economy. The impacts through the supply chain therefore would be expected to reduce the UK's overall level of GVA.

The potential impact on the UK economy of the cyber incident to the rail network as a result of lost output among businesses and the impact on their supply chains has been estimated using an Input-Output methodology[134] using sector-specific Type I multipliers[135] derived from ONS Input-Output tables.[136] These have been applied to direct GVA impacts estimated for the rail sector (train and freight operators) prior to compensation[137], and construction sector. The wider economic impact associated with lost working days for business has not been estimated due to uncertainty as to the sectors that will be impacted. However, based on the estimated direct GVA impact reported in Section 5.4.1, this wider impact is likely to be small.

It is estimated that the wider economic impact through the supply chain resulting from the week-long disruption to the rail network could be up to £760.1 million. This impact is largely driven by the supply chain effects associated with the potential GVA reduction in the construction sector through disrupted

[132] Sourced from ONS Supply and Use tables: ONS (2024) Input-Output analytical tables - Office for National Statistics
[133] ORR, 2025 Table 1314 - Freight moved by commodity (periodic) | ORR Data Portal
[134] Input-Output tables show, in matrix form, the inter-linkages between sectors of the economy in terms of the value of goods and services (inputs) that are required to produce each unit of output in given sectors of the economy.
[135] Type I multipliers include the impact on production of a change in final use (direct impact) and the supply chain impacts stemming from the initial change in final use (indirect impact).
[136] ONS (2024) Input-Output analytical tables - Office for National Statistics
[137] Whilst operators will be compensated for their losses, there will be an economic impact on the wider supply chain due to the reduction in their activity over the period of disruption. The wider supply chain impact is therefore estimated based on their implied reduction in GVA.

freight. It should be considered to represent an upper end estimate in terms of potential scale of impact.

It should be noted that, by nature, Input-Output methodologies are static and do not capture the dynamic impacts that may result from changes in behaviour or actions in response to a shock to the economy. The estimated wider economic impact therefore only provides a short-run view of the potential impact on UK GVA. However, given the short term and relatively limited nature of impacts expected from the cyber incident scenario, any longer term impact of the scenario is expected to be very limited.

5.6 Summary of the economic impact on industry, business, consumers and wider economy

Drawing on the results of the direct financial impacts, indirect economic impacts and wider economic impacts set out in Section 4 and 5, Table 4 below presents a summary of the quantified economic impacts of a systemic cyber incident to the rail network.

In total, it is estimated that the systemic cyber incident to the rail network could result in a total economic cost of approximately £1.8 Billion for a weeks period of disruption. This includes a financial cost to Network Rail in the region of £123.0 million, a cost to passengers of delays of £281.3 million and a potential GVA impact of up to £1,397.0 million. Put in context, the estimated GVA impact represents approximately 2.8% of the UK's total GDP per week, and 0.05% of annual GDP.

Given the relatively short period of disruption and small estimated economic impact, longer term economic impacts would not be expected. Furthermore, the GVA impact is largely driven by the estimated impact of supply chain disruption which, based on the approach taken to estimating this, is considered to reflect the upper end in terms of scale of potential costs. Indeed, given the number of factors that will influence the scale of impact of a cyber attack on the rail sector, all figures should be considered indicative only.

Table 4: Summary of the direct and indirect economic impacts of a systemic cyber incident to the rail network

Impact type	Stakeholder impacted	Impact area	Estimated economic impact (£ million, 2024 prices)
Direct	Network Rail	Direct financial cost to organisation (a)	£123.5
Indirect	Train and freight operators[138]	Cost of lost output (GVA) (b)	£0
	Passengers/consumers	Cost of longer journey times (c)	£281.3
	Businesses	Productivity impact of lost work days (GVA) (d)	£116.7
		Cost of lost output due to supply chain (freight) disruption (GVA) (e)	£520.1[139]
Wider economic impacts		Wider supply chain impact of reduction in output (GVA) (f)	£760.1
Total GVA impact (excludes consumer impacts, therefore equal to b, d, e, f)		The productivity impact of lost work days, cost of lost output due to supply chain disruption and wider supply chain impact.	£1,397.0
Total Economic Cost (a,b,c,d,e,f)			£1,801.7

Source: KPMG analysis

In addition to the monetary impacts presented in Table 4 above, there are a number of impacts that have not been quantitively assessed as part of this study. These additional impacts have been assessed in qualitative terms, drawing on available evidence. These qualitative assessments are included throughout Sections 5.2, 5.3 and 5.4. To the extent to which these additional impacts materialise as a result of the systemic cyber incident to the GB rail network, they would add to the quantified economic impacts shown in the table above.

[138] While train and freight operators are expected to be affected by the cyber attack through loss of revenues, their contracts with Network Rail mean that they would be compensated for any losses by Network Rail – the costs of which are included in Network Rail's direct financial costs.
[139] Ibid.

6 Assessment of the likelihood of a systemic cyber incident to the GB rail network

6.1 Introduction to the section

Alongside assessing the impact of a systemic cyber incident on the rail sector, the likelihood of such an incident occurring is also considered

Assessing the likelihood of a systemic cyber incident impacting the rail sector is a complex task. Unlike traditional cyber threats that target individual systems or organisations, a systemic cyber incident poses a broader threat to the entire infrastructure and its interconnected functions. Recent supply chain incidents such as Log4j Vulnerability (2021), SolarWinds (2020), CrowdStrike Update (2024), and Facebook Outage (2021)[140] highlight the growing frequency and impact of major cyber incidents affecting a range of sectors. In such cases, the impact of these incidents was amplified by interdependencies with third party suppliers and resulted in rapid escalation across sectors and geographies. These incidents illustrate the growing likelihood of a systemic cyber event impacting multiple sectors, including the rail industry.

However, the complexity of cyberspace, and the multiple factors that determine systemic risk, makes its assessment challenging. Specifically, assessment of systemic risk requires and understanding of the threat itself but also the context in which any potential incident could result in a systemic incident – including consideration of the interconnectedness of systems, overlapping infrastructure and the potential for cascading failures.

These components are considered in the assessment of the likelihood of a systemic cyber incident in the rail sector, covered in the Section 6.2-6.5 below. This provides a high-level qualitative assessment based on data available through open-source materials and KPMG insights regarding the maturity of cyber security controls and common vulnerabilities across the rail sector.

6.2 Assessment approaches

There are a number of approaches identified that can be used to assess systemic cyber risk. Existing approaches, typically applied in the financial services sector or in national security frameworks, focus on identifying critical functions, analysing interdependencies, and evaluating vulnerabilities. Such approaches include the following:

- Financial System Focus: The financial sector has been at the forefront of systemic risk analysis, with organisations like the European Systemic Risk Board (ESRB) developing frameworks to assess how cyber incidents could trigger a systemic crisis. These frameworks often focus on the interconnectedness of financial institutions and the potential for cascading failures.[141]

- National Security Perspective: Organisations like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and UK National Cyber Security Centre (NCSC) have adopted a national security perspective, focusing on cyber risks that pose critical threats to the nation's security and economic security. They have adopted cybersecurity frameworks that provide a structured approach to assessing and managing cyber risks. These frameworks often include a risk assessment process that considers likelihood, impact, and vulnerabilities.[142]

[140] The Register (2024). How did a CrowdStrike file crash millions of Windows computers?
[141] ESRB (2020). Systemic Cyber Risk.
[142] CISA (2025). Risk Management; NCSC (2025). Risk Management.

— Insurance Industry Approach: The insurance industry has also developed approaches to assess systemic cyber risk, particularly in the context of uninsurable events. They consider the scale of potential losses, loss correlation across sectors, and the difficulty of modelling and hedging.[143]

The cyber security frameworks of CISA and NCSC are limited to the organisation or entity level approach to assessing risk and do not account for the interconnectedness of entities, common vulnerabilities or overlapping infrastructure – factors that must be assessed to understand the likelihood of a systemic cyber incident occurring.

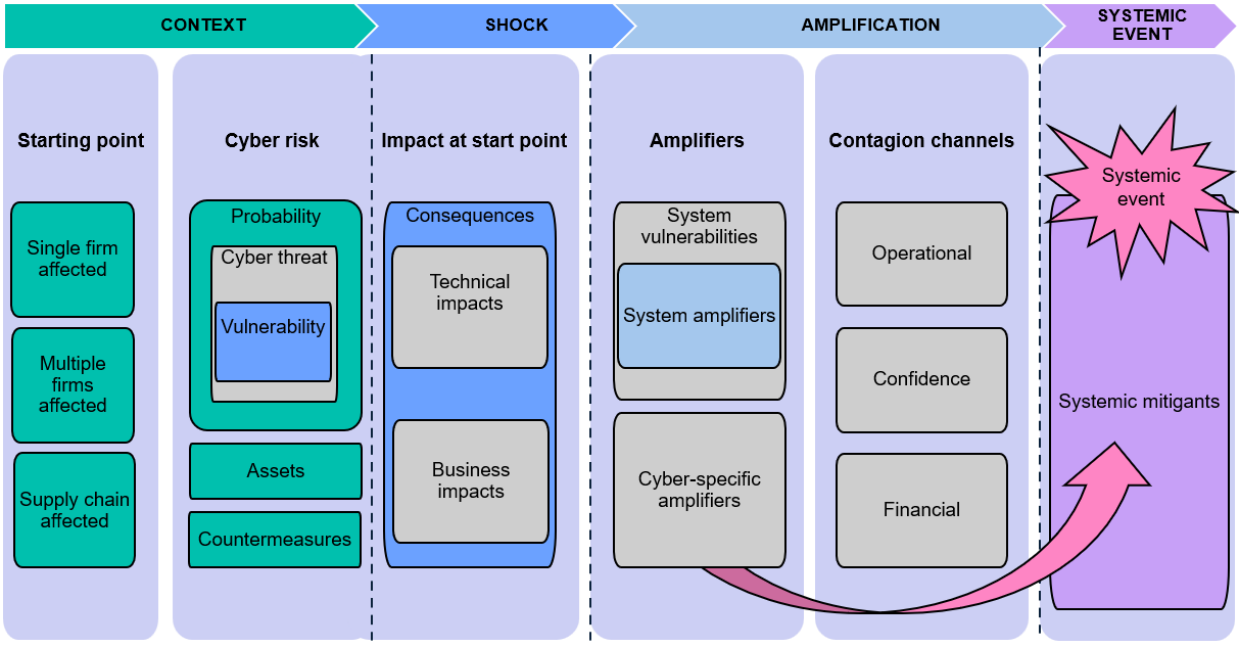
Financial services and insurance sector frameworks provide more appropriate models for assessing the likelihood of a systemic cyber incident. These approaches account for the rail sector's interconnectedness and the potential for cascading failures, allowing for a more comprehensive understanding of how a cyber incident could escalate into a systemic event. The ESRB provides a comprehensive, repeatable model that focuses on identifying vulnerabilities that amplify the shock of a cyber incident and understanding when an incident might become systemic provides a valuable framework for developing effective mitigation strategies. The ESRB's framework developed by its European Systemic Cyber Group (ESCG) to analyse systemic cyber risk to the European financial system has therefore been selected for application in this study. When the conceptual model was published, no cyber incidents leading to a systemic impact on the financial system had materialised. As such, the model considers whether cyber risk has the potential to trigger serious and systemic financial repercussions, and how this might happen.

6.3 Framework for assessment

6.3.1 Overview of framework

The ESCG provides a structured methodology for analysing cyber incidents in four distinct 'phases': context (cyber risk), shock (impact at start point), amplification, and systemic event.

Figure 3.1: ESRB Systemic Cyber Risk Conceptual Framework



Source: ESRB

More detail on each phase is provided below along with their mapping to the threat landscape as it applies to the rail sector. This mapping has been used to provide an assessment of how the rail

[143] AIG (2017). Is Cyber Risk Systemic?

sector would perform at each phase based on threats to its networks, cyber maturity of the sector, likely impact, and amplification factors.

6.3.2 Phase 1: Context

Within the ESRB framework, context refers to the circumstances in which a cyber incident arises in the form of a crystallised cyber risk. This phase examines the constituent parts of cyber risk which provide the setting and origin for a potential cyber incident and can be broken down into:

— the starting point for an incident; and

— cyber risk, considered in terms of probability, assets and countermeasures.

Each is considered below.

Starting Point

The starting point considers the types of cyber events impacting the rail sector that could initiate a systemic disruption resulting in widespread impact, affecting multiple organisations, industries, or even entire nations. It is not just about a single company losing data or facing downtime but the domino effect that ripples through critical infrastructure, financial systems, and global supply chains. This type of incident would begin with an incident impacting a single organisation or multiple organisations at the same time, or an incident where the initial attack vector comes via the supply chain. Elements in the following three phases (shock, amplification, systemic event) would need to be present for escalation to a systemic incident.

Cyber Risk

This element considers the risk of a cyber event occurring. It examines:

3) The probability of a successful attack, including:

    a. cyber threat, including capabilities and motivations of attackers; and

    b. vulnerability to attack.

3) Assets that may be put at risk as a result of the attack such as supervisory control and data acquisition (SCADA) systems, operational technology (OT) networks, financial systems, or enterprise IT.

3) Countermeasures that may be put in place by organisations and policymakers to mitigate cyber risk.

These are assessed in turn below and together inform an assessment of the cyber risk associated with a systemic cyber incident as part of Phase 1 of the ESRB model.

1) Probability of a successful attack

a. Cyber Threat

Cyber threat refers to the types of threats, their capabilities and motivation for targeting the rail sector. Potential motivations for attack on the rail sector are considered below.

– Financial Gain: Ransomware attacks are often motivated by financial gain, as attackers demand payment from victims to restore access to their systems. Such a threat could target critical systems, demanding payment, and potentially causing widespread service outages.

E.g. Skånetrafiken (2021), a ransomware attack, disrupted ticketing systems and caused significant service disruptions for the Swedish public transport operator.[144]

- Political Disruption: Hacktivist groups may target railway systems to disrupt transportation services and cause political instability. DDoS Attacks could overload systems with traffic, causing denial of service and disrupting operations. E.g. In 2022, in an attack on the Belarusian Railway, hacktivists launched a ransomware attack to disrupt Russian troop movements, targeting the Belarusian state-run train company.[145]

- Supply Chain Compromise: Exploiting vulnerabilities in third-party suppliers, impacting the availability of essential components or services. E.g. In 2022, a Distributed Denial of Service (DDoS) attack on a third-party ICT service provider disrupted operations for the Danish train operator DSB. [146]

- Accidental Compromise of Systems: The Facebook and CrowdStrike incidents demonstrate how code errors or mistakes in software updates can lead to indiscriminate service outage across a range of sectors and services. Network Rail reported a number of train operating companies were affected by the CrowdStrike code misconfiguration error which impacted global transport systems: Avanti West Coast, c2c, Gatwick Express, Great Northern, Great Western Railway, Hull Trains, London Northwestern Railway, Lumo, Merseyrail, Northern, Southern, Thameslink, Transport for Wales, TransPennine Express, West Midlands Railway were affected.[147] The issue impacted ticketing machines, the systems for which were highly likely provided by a third-party supplier to these railway companies, which were, in turn, impacted by a code misconfiguration in their own supply chain caused by a Crowdstrike cybersecurity product.[148]

Each of the above threats could lead to cyber incidents resulting in significant operational downtime, data-loss, or physical damage. It would be necessary for factors described in the Amplification phase (see 6.4) to be present for such an incident to escalate into a systemic event. As the Colonial Pipeline incident suggests, the threat actor responsible would not necessarily intend to cause such widespread harm. There is, therefore, a risk that the impact of a cyber incident could cascade to systems beyond its original target. This could lead to a systemic event occurring accidentally. Countermeasures at a technical, organisational and institutional level must be in place to mitigate the risk of amplification factors and prevent escalation into a systemic event.

b. Vulnerability to attack

The frequency with which cyber attacks have impacted rail systems has increased by more than 200% in the last five years. In 2024, Colonel Cedric Leighton, CNN Military Analyst reported, "We've seen a 220% increase in railway-associated cyber attacks over the last five years… In fact, over a 10-year period, we've seen cyber incidents impacting railway systems in countries as diverse as Belgium, France, Poland, the Czech Republic, Germany, Denmark, Italy, Belarus, Ukraine, India, and the United States. So, this is clearly a worldwide problem."[149] The Skånetrafiken, Belarusian Railway, Danish Railway, and CrowdStrike incidents evidence the rail sector's growing vulnerability to cyber incidents. This trend is highly likely to continue as rail networks and train operators rely on growing interconnectivity of services. The CrowdStrike incident highlights the increasing threat of cyber incidents impacting all sectors due to the growing interconnectedness of organisations due to overlap in suppliers and interdependencies. Other recent events demonstrate the growing frequency and impact of supply chain incidents where a third-party supplier has been deliberately targeted by malicious threat actors seeking to capitalise on the omnipotence of a particular software to target a

[144] ENISA (2020). Railway Cybersecurity.
[145] IRJ (2023). EU cybersecurity agency reports on threat to rail.
[146] Infosecurity Magazine (2018). Danish Railway Company DSB Suffers DDoS Attack.
[147] The Mirror (2024). Full list of UK train lines hit by IT outage as services cancelled and ticket machines stop working.
[148] Railway Technology (2024). Global transport systems struck by IT failure.
[149] Secureworld (2024). Cyber Attacks on Railway Systems Increase by 220%.

broad spectrum of victims motivated by financial gain or intelligence gathering operations. Below is a list of incidents impacting the rail sector in recent years that highlight the sector's vulnerability to cyber attacks.

- NotPetya (2017): This ransomware attack, attributed to a Russian state-sponsored group, spread through a Ukrainian accounting software called M.E.Doc. The Russian threat actor that deployed this malware originally only intended to target this specific software in Ukrainian computers, yet went on to cause 10 billion USD in damage globally, impacting businesses and critical infrastructure, including some railway systems. [150]
- SolarWinds (2020): A Russian state-sponsored group compromised SolarWinds, a software company that provides IT management tools to thousands of organisations, including government agencies and critical infrastructure providers. This attack allowed the attackers to gain access to sensitive data and potentially disrupt operations.[151]
- Microsoft Exchange (2021): A Chinese state-sponsored group exploited vulnerabilities in Microsoft Exchange Server, allowing them to gain access to email accounts and potentially steal sensitive information or disrupt operations.[152]
- Salt Typhoon, Volt Typhoon (2020-present): Chinese-nexus threat actors have also been observed targeting CNI organisations with the objective of prepositioning within the victim network. It is highly likely this activity is motivated by real-world political and military events and would likely result in real-world impact in the event of escalating political tensions.[153]

There are emerging threats and vulnerabilities specific to the rail sector, such as the increasing use of connected trains, autonomous systems, and reliance on cloud services. Key vulnerabilities in the rail sector include:

- Connected Trains: The increasing use of connected trains, which rely on wireless communication and data exchange, creates new attack surfaces for cybercriminals.
- Autonomous Systems: The development of autonomous train systems raises concerns about the security of the software and algorithms that control these systems.
- Cloud Services: The rail sector's increasing reliance on cloud services for data storage, processing, and applications increases the risk of data breaches and service disruptions.
- Third-party vendors: Which, in some cases, are concentrated on a particular supplier of software or infrastructure. If such a service were vulnerable to an attack or compromised, it would impact more than one train operator or rail service.
- Legacy Systems: Many rail companies still rely on legacy systems that are difficult to secure and update. These systems are often vulnerable to known exploits and can be a gateway for attackers to gain access to the network.

In summary, the rail sector is increasingly exposed to a range of sophisticated threat actors from nation state to financially motivated ransomware groups. This is the result of ongoing and escalating geopolitical tensions in Europe. In addition, the sector is vulnerable to cyber attacks due to issues concerning legacy infrastructure, interconnectedness, supply chain dependency, and unsecured OT networks.

[150] Brookings (2021). How the NotPetya attack is reshaping cyber insurance.
[151] NCSC (2021). NCSC Annual Review 2021.
[152] CISA (2024). Review of the Summer 2023 Microsoft Exchange Online Intrusion.
[153] NCSC (2024). NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks.

2) Assets

Assets refers to non-financial assets such as hardware, software, intellectual property, etc. Railway assets encompass a wide range of components, including physical infrastructure like tracks, buildings, and signalling systems, as well as digital assets such as servers, databases, applications, and even personnel. These assets are susceptible to vulnerabilities, which represent potential weaknesses that threat actors, including individuals, organisations, and nation-states, can exploit to cause harm. Digital assets, as defined by Carroll et al., encompass any digital information owned by an individual, whether stored locally on a personal device or remotely accessed through contractual agreements.[154] This broad definition includes data stored online, such as social media profiles and website content, often referred to as "cloud" storage.

It is important to understand which cyber incidents have the potential to put life at risk or lead to the greatest disruption to network rail or train operator services. This can be done by identifying the high-level systemic functions of the railway services and draw high-level linkages between these critical functions and related assets. ENISA[155] highlights eight key functions of rail operators[156] which are presented below with the high level linkages to assets identified:

- Operating traffic on the network: This function relies on assets such as signalling systems, track control systems, and communication networks. Failure of these systems could impact passenger safety resulting in a threat to life.[157]
- Ensuring safety and security: This function relies on assets such as CCTV systems, emergency response systems, and security protocols.
- Maintaining railway infrastructure and trains: This function relies on assets such as track maintenance equipment, rolling stock, and maintenance databases.
- Managing invoicing and finance: This function relies on assets such as financial systems, payment gateways, and accounting software.
- Planning operations and booking resources: This function relies on assets such as scheduling software, resource management systems, and operational databases.
- Information for passengers and customers: This function relies on assets such as websites, mobile apps, and customer service systems.
- Carrying goods and passengers: This function relies on assets such as trains, locomotives, and rolling stock.
- Selling and distributing tickets: This function relies on assets such as ticketing systems, fare collection machines, and revenue management software.

It is necessary to prioritise securing these critical assets and implement robust cybersecurity measures to mitigate greatest risk to rail network operations and passenger safety. The safety of passengers could be at risk in the event of an incident impacting cloud services. For example, Sweden's railway system uses a cloud service to process data about its infrastructure and rolling stock. This data fuels advanced maintenance strategies, such as predictive maintenance and Condition-Based Maintenance (CBM). CBM, in particular, uses real-time asset condition data to anticipate potential failures and target maintenance efforts only on affected components. This real-

[154] Carroll EE et. al. (2011). Helping clients reach their great digital beyond.
[155] The EU agency dedicated to enhancing cybersecurity in Europe.
[156] ENISA (2020). Railway Cybersecurity.
[157] Ravdeep Kour et. al. (2022). A review on cybersecurity in railways.

time monitoring of aging infrastructure through digital technology offers significant benefits for railway organisations. It allows for more efficient maintenance, repair, and operations, ultimately improving safety for employees, passengers, and the environment. The collected data is fed into analytical engines to generate predictions, such as forecasting the condition of tracks. While this data-driven approach offers numerous advantages, it also raises security concerns for society. These concerns are not hypothetical, as numerous railway organisations relying on digital infrastructure have faced cybersecurity attacks. [158] Cloud services and assets such as CBM that are widely used across Network Rail, or its train operators present widespread risk to the sector if compromised.

2) Countermeasures

Countermeasures are the methods present that organisations and policymakers implement to mitigate cyber risk. These countermeasures can be categorised into legal, technical, organisational and institutional level measures.

- Legal countermeasures: The UK Government has enacted several laws and regulations to address cybersecurity:
- The Department for Transport (DfT): acts as lead on enforcing Network and Information Systems (NIS) Regulations 2018 that implements the EU NIS Directive across the rail network[159], requiring organisations in critical sectors to implement cybersecurity measures and report incidents.
- The Office of Rail and Road (ORR): ensures that UK railways are safely regulated particularly as railways become more digitised, with an increasing focus on cybersecurity implications for passenger safety. Safety risks caused by poorly designed, operated, and maintained software-based systems are within the remit of ORR. The ORR works with regulators and railway industry experts to conduct a risk assessments and prioritise targeting of resources.[160]
- Data Protection Act 2018: requires organisations to protect personal data and report data breaches. Non-compliance can lead to hefty fines and operational sanctions, so railway operators must prioritise meeting these regulatory requirements. [161]
- Technical countermeasures: UK rail sector is taking steps to improve its cyber security posture. However, there is still work to be done to address the challenges posed by legacy systems, supply chain risks, and increasing interconnectivity of systems, and connectivity between OT and IT networks. This will be explored in further detail in Phase 3 - Amplification.
- Organisation level countermeasures: at an organisational level, the rail sector is taking steps to mitigate risks by implementing strategies in line with the NIS2 directive.[162] Measures being taken include risk assessment and management, security controls (firewalls, intrusion detection, and access control measures), incident response plans, staff training, supply chain management, and collaboration and information sharing with government agencies to share best practices on cyber security.

In summary, the UK rail sector is taking steps to mitigate cyber risk through legal, technical, and organisational countermeasures. The government has implemented regulations like the NIS Regulations and Data Protection Act, while industry bodies have developed cybersecurity standards and best practices. Companies are investing in new technologies and risk mitigation strategies, but challenges remain, including legacy systems and interconnected networks.

[158] Ravdeep Kour et. al. (2022). A review on cybersecurity in railways.
[159] UK HMG (2018). The NIS Regulations 2018.
[160] ORR (2025). Keeping Britain's railway safe from cyber threats.
[161] UK HMG (2018). UK Data Protection Act 2018.
[162] ENISA (2025). Network and Information Systems Directive 2 (NIS2).

Summary of Phase 1 assessment

It is highly likely the rail sector will be subject to a cyber incident impacting on its operational resilience in the next 1-2 years. This assessment is based on recent incidents, and common vulnerabilities across organisations in the sector, as well as related countermeasures. Recent cyber incidents impacting the ticketing systems have led to service outage of rail services in Europe and the UK. The sector has been targeted by financially motivated threat actors as well as politically motivated groups seeking to disrupt operations. In addition, there has been a growing number of supply chain incidents impacting organisations globally such as the CrowdStrike code error that led to outages across the rail network in the UK and Europe. Supply chains are becoming more complex, and threat actors are exploiting vulnerabilities in widely used systems to gain onward further access to indiscriminately target victim organisations. There is also an ongoing and increasing likelihood of state-sponsored activity targeting rail networks and infrastructure due to geopolitical tensions in Russia and the China region

6.3.3 Phase 2: Shock

The shock phase describes the immediate technical and business impacts experienced at the point when the cyber incident has its initial impact. This phase focuses on the impact or consequences (as opposed to the likelihood of the shock). The conceptual model further distinguishes between technical and business impacts, thereby capturing the link between the loss of cybersecurity properties for the assets affected and the first-order effects of this disruption for the affected institution(s).

As an illustration of the potential scale of impact of a cyber attack on the rail sector, according to the UK Government's National Risk Register (NRR)[163], cyber attacks on the UK transport sector pose a significant threat to the economy, public safety, and national security. It notes that system recovery could take hours to months, depending on the nature of the attack. Disruptions to critical goods supply chains would require a tailored response to ensure the effective movement of goods, and the cost of recovery could reach millions.[164]

Previous incidents highlight the range of impacts of cyber incidents on railway companies including disruption to operational resilience, financial and data loss, regulatory fines due to data breaches and non-compliance. Impacts caused by the CrowdStrike, Not Petya, and SolarWinds incidents resulted in service disruptions and data breaches and significant financial losses. For example, the CrowdStrike incident led to service disruption for rail services across Europe and the UK[165]. Volt Typhoon and other Chinese-nexus threat actors have also been observed targeting CNI organisations with the objective of prepositioning within the victim network.[166] Other incidents such as the Colonial Pipeline incident[167] and Russian activity targeting Ukrainian CNI[168] demonstrate threat actor capabilities in gaining access to OT networks and causing real-world damage to CNI.

Russia's war with Ukraine has also highlighted the vulnerability of rail networks to cyber attacks: hackers from the Ukrainian intelligence agency targeted Russian company Region Trans Service LLC resulting in destruction of all the company's servers and ticketing systems and online services being taken offline for several hours.[169]

In summary, the increasing integration of IT and OT systems in railways creates new vulnerabilities for cyber attacks, potentially disrupting train operations and even causing accidents.

[163] HMG (2025). National Risk Register 2025.
[164] HMG (2025). National Risk Register - 2025 edition.
[165] Railway Technology (2024). Global transport systems struck by IT failure.
[166] Microsoft Security Blog (2023). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.
[167] CISA (2021). The Attack on Colonial Pipeline.
[168] NCSC (2024). Heightened threat of state-aligned groups against western critical national infrastructure.
[169] The Record (2023). Russian railway site allegedly taken down by Ukrainian hackers.

Summary of Phase 2 assessment

A cyber incident in the rail sector can have a devastating impact, disrupting operations, causing financial losses, and potentially leading to a systemic crisis. The initial shock phase involves immediate technical and business disruptions, affecting operational resilience, data integrity, and financial stability. Examples such as the CrowdStrike incident demonstrate the potential for widespread service disruptions across entire rail networks.

The increasing integration of IT and OT systems in railways creates new vulnerabilities, making them susceptible to attacks that can disrupt train operations and even cause accidents. Russia's war in Ukraine highlights this vulnerability, with incidents like the targeting of Region Trans Service LLC demonstrating the potential for real-world damage to rail infrastructure.

With amplification factors present, such as those listed in Phase 3 below, a cyber incident on the rail sector could propagate beyond the targeted company to impact passengers, freight transport, and the broader economy. The government's response, whilst crucial, may be insufficient to mitigate the full impact, highlighting the need for robust cybersecurity measures and coordinated efforts across the industry.

6.3.4 Phase 3: Amplification

The amplification phase explores the interactions between the affected institutions and the systems which they use, and the factors that influence how shocks propagate through these systems. In this phase, the conceptual model brings together two concepts: 1) amplifiers, which if present are likely to increase the probability or consequences of the shock; and 2) contagion channels, which transmit the shock through the systems. These concepts are discussed regards the rail sector in detail below.

Amplifiers

Systemic and cyber-specific vulnerabilities will determine to what extent an incident in one part of the railway system could cascade and impact other critical functions. The types of vulnerabilities that could amplify the impact of a cyber incident in the rail sector include lack of cybersecurity awareness, insufficient investment in cybersecurity, legacy systems, complex interconnections.[170] The intricate web of systems and dependencies can make it challenging to contain a cyber incidents and response capabilities. As such, cyber incidents (or triggers) could propagate through the rail sector's interconnected systems and interdependencies.

Contagion channels

The rail sector is highly interconnected, both internally (IT and OT systems) and externally (supply chains and other critical infrastructure). Disruptions in one area can cascade and impact others, including through the following routes:

- IT and OT systems: A cyber attack on a railway's IT network could disrupt the flow of information to operational control systems, leading to delays or disruptions in train operations. The increasing integration of IT and OT systems creates new attack surfaces, potentially allowing attackers to manipulate control systems or disrupt critical processes.
- Network infrastructure: A cyber attack on a railway's communication network could disrupt signalling systems, leading to train collisions or derailments. Vulnerabilities in network protocols, devices, and configurations could allow attackers to spread malware or disrupt communications.
- Supply chains: A cyber attack on a supplier of railway equipment or software could disrupt the production and delivery of essential components, leading to delays or disruptions in service.

[170] Based on KPMG insights.

Compromises in supplier networks could lead to the introduction of malicious software or hardware into the railway system.

- Other Critical Infrastructure: A cyber attack on a power grid could disrupt electricity supply to railway systems, leading to service outages.

Summary of Phase 3 assessment

In summary, there are several amplification factors that could exacerbate the impact of a cyber attack on a railway network. These factors include the increasing integration of IT and OT systems, creating new attack surfaces for malicious actors. Vulnerabilities in network infrastructure, particularly signalling systems, could lead to catastrophic consequences like collisions. Furthermore, compromised supply chains could introduce malicious software or hardware into the railway system, whilst disruptions to other critical infrastructure, like power grids, could cause widespread service outages. These interconnected vulnerabilities and dependencies create a complex web of potential amplification factors, making cyber attacks on railway networks particularly dangerous.

6.3.5 Phase 4: Systemic event

The systemic event examines the point at which the system is no longer able to absorb the shock. The ESRB framework defines an "impact tolerance threshold" as the upper limit of a system's ability to withstand shocks without experiencing a cascading failure. The "absorptive capacity" is the gap between this threshold and a lower bound, representing the system's resilience.

Below are some example cybersecurity standards and information sharing that are 'legal countermeasures' that mitigate the risk of systemic event impacting the rail sector as based upon KPMG cyber expertise. These measures are at an institutional level. Actions taken by the government to specifically mitigate the risk of an organisational level cyber attack could spread to impact the rail sector at a systemic level:

- Cybersecurity Standards: Mandating robust cybersecurity standards for all rail companies, including suppliers, to ensure a secure and resilient network. With the UK rail industry, it has made significant progress in implementing cybersecurity standards. Network Rail and train operators have adopted industry-specific standards like the Railway Safety and Standards Board (RSSB) guidelines and the NCSC guidance. Challenges arise in maintaining a consistent level of cybersecurity across the entire rail ecosystem, including smaller suppliers and contractors, remains a challenge.

- Information Sharing: Establishing a framework for sharing cyber threat intelligence and best practices among rail companies, government agencies, and industry partners. UK rail sector information sharing is improving, with initiatives like the Rail Industry Cyber Security Forum (RICSF) facilitating collaboration and knowledge exchange. There still exists challenges in sharing sensitive information, particularly about vulnerabilities and incidents, can be challenging due to concerns about competitive advantage and legal liabilities.

Summary of Phase 4 assessment

In summary, the UK rail industry is making progress in implementing cybersecurity measures, but there is still room for improvement. The industry needs to continue to invest in cybersecurity, enhance information sharing, strengthen supply chain security, and implement more robust network segmentation and redundancy measures. It is important to note that this is a general assessment, and the maturity of individual companies within the UK rail sector can vary significantly.[171] The maturity of these practices in the rail sector will determine its "impact tolerance threshold" to withstand shocks without experiencing a cascading failure.

[171] See websites for: NCSC, DfT, Rail Industry Cyber Security Forum (RICSF), Association of Train Operating Companies (ATOC), UCL papers on cybersecurity and transportation, papers on cybersecurity of rail systems.

6.4 Likelihood assessment

Below is a summary of the UK rail network's cybersecurity posture mapped against the four phases of the ESRB model: Context, Shock, Amplification and Systemic Event.

- Context: There have been several recent cyber incidents impacting the rail networks of the UK and Europe that have led to service outage, as detailed in Phase 1 of this assessment. These include financially motivated threat actors as well as politically motivated groups seeking to disrupt operations. In addition, there has been a growing number of supply chain incidents impacting organisations globally such as the CrowdStrike code error that led to outages across the rail network in the UK and Europe. Organisations' supply chains are becoming more complex, and threat actors are exploiting vulnerabilities in widely used systems to gain onward further access to indiscriminately target victim organisations. In this context, it is highly likely the rail sector will be subject to a cyber incident impacting on its operational resilience over the next 2 years.

- Shock: The impact of an incident can be determined by the services affected. The shock would be greatest if the systems listed in ENISA's list of "Eight Key Functions" of the railway were affected, which could lead to operational impact on delivery of services due to downtime in IT systems, ticketing and payment systems and OT networks. Recent incidents involving rail sector organisations have largely impacted ticketing and payment systems resulting in disrupted services or return to manual ticketing processes.

- Amplification: There exist significant numbers of interconnected systems and interdependencies within the rail sector that could amplify the impact of a cyber incident to the extent it could result in a systemic event. This is due to internal and external interconnections and dependencies that could lead to a cascade effect across the victim organisation's supply chain.

- Systemic event: The UK rail industry is making progress in implementing cybersecurity measures, but it is still a work in progress. Whilst Network Rail and train operators have adopted industry standards and are investing in cybersecurity, there is room for improvement in several areas. The industry has made strides in adopting cybersecurity standards and investing in security measures but there is a need to enhance information sharing, strengthen supply chain security, and implement more robust network segmentation and redundancy measures. The maturity of cybersecurity practices varies significantly among individual companies within the rail sector. The maturity of these practices will directly impact the rail sector's "impact tolerance threshold," which is its ability to withstand shocks without experiencing a cascading failure. In summary, the UK rail industry is making progress in these areas but needs to continue its efforts to build a more robust and resilient cybersecurity posture to protect against the growing threat of cyber attacks.

For this likelihood assessment of a systemic cyber incident impacting the UK rail sector, the risk of a malicious threat actor conducting a successful attack, is balanced against an assessment of the vulnerability potential targets are to an attack, amplification factors, as well as institutional, legal and regulatory countermeasures in place. These 4 parameters, informed by the above qualitative assessments and insights in Section 6.3, are collated together to form one likelihood score. Evidence mapped against ESRBs conceptual framework leads to an assessment that there is a low likelihood that within a 2 year period a cyber incident targeting the UK rail sector will result in systemic level impact leading to significant disruption of rail services.

Recent incidents in the UK and Europe show that one of the most common assets targeted in the rail sector are ticketing systems. These incidents however have an isolated financial impact on victim organisations as factors leading to systemic event are not present. In war zones such as Ukraine and Russia, rail service providers are targeted by state sponsored groups and hacktivists seeking to gain

political capital and disrupt operations. It is unlikely the UK rail network is a target of these groups, but this status could change with evolving geopolitical events in Europe, and globally.

The widespread impact of recent incidents has been mitigated by security controls and cyber maturity of organisations in the rail sector as well as national level policies promoting cybersecurity practices such as regulatory enforcement, information sharing and education. It is important to note that cybersecurity maturity is not consistent across the sector and there remains a risk an incident could occur in a single organisation and spread to other organisations. Further, this assessment should be reviewed over time as changes to the threat landscape occur. As such, continued monitoring of the above factors is recommended to ensure the likelihood scoring remains accurate for future assessments.

Appendix 1: Literature review protocol

The table below details the literature review protocol used for the systematic literature review undertaken by Madeline Carr and Filippo Gualtiero Blancato, University College London (UCL), Department of Computer Science.

Title	A Systematic Review of the Societal and Economic Impact of Cyber Incidents in the Rail Transport and Gas Sectors.
Summary	As the rail transport and gas sectors become increasingly digitised, they become valuable targets for cyber attacks and related cyber incidents. Given the importance of these sectors for the global economy and the complexity of their infrastructures, it is important to understand the characteristics of such cyber attacks and their impact. Evidence from the literature suggests that attacks on the rail and gas sector can disrupt operations and may result in significant financial loss. Moreover, some categories of attacks can be hard to detect, making it more challenging to mitigate their risks. In this review, studies about the cybersecurity challenges facing the rail transport and gas sector are reviewed and their societal and economic impact considered.
Research questions	1. What are the specific impacts if the critical sector is victim to a cyber attack compared to a conventional attack? 2. Where are the economic impacts felt across businesses and consumers? 3. What are the economic costs of the attack? This includes both direct (e.g. immediate financial losses and recovery costs); and indirect costs (e.g. those resulting from reduced investments; and reduced consumer confidence in the sector). 4. What is the best methodology to model?
Databases	Electronic databases to be searched: — Web of Science (Databases covered: Conference Proceedings Citation Index, Science Citation Index Expanded, Social Sciences Citation Index, Arts & Humanities Citation Index, and Book Citation Index) — ACM digital library (comprehensive database of full-text articles and bibliographic literature covering computing and information technology from Association for Computing Machinery publications) — IEEE Xplore (indexed articles and papers on computer science, electrical engineering and electronics from the Institute of Electrical and Electronics Engineers (IEEE) and the Institution of Engineering and Technology) * — Scopus (Elsevier's abstract and citation database - Content on Scopus comes from over 5,000 publishers and must be reviewed and selected by an independent Content Selection and Advisory Board (CSAB) to be, and continue to be, indexed on Scopus) — Google Scholar: search engine that indexes the full text or metadata of scholarly literature, both peer reviewed and pre-print. Studies that are too broad, irrelevant, and/or duplicates of other results will be excluded.
Inclusion criteria	— Academic literature (peer-reviewed) — Grey literature ((industry reports, policy briefs, government/international organisations/NGOs publications). Studies must discuss cyber attacks and related cyber incidents to the rail transport and gas sectors, as well as their impact. For reasons of time and scope, only articles published since 2012 and published in English are included.

Literature search strategy	Searches will be conducted in the above databases for papers published between 2012 and 2022. Search terms: “cyber incident*” OR “cyber attack*” OR “cyber security” OR “incident” AND “cost*” OR “socio-economic cost*” OR “damage*” OR “financial cost*” OR “financial harm” OR “financial loss” OR “economic loss” OR “estimate*” OR “outage” OR “loss of life” OR “societal implication*” OR “disruption*” OR “soc* impact” OR “soc* implication*” AND “rail” OR “gas” OR “rail transport” OR “gas sector” OR “rail sector” OR “rail and gas” OR “critical national infrastructure” Forward and backward searches from the references of papers found through the database search to identify additional relevant studies will be conducted.
Piloting	Search terms have been piloted on the databases listed above to retrieve a high proportion of relevant articles and a low proportion of irrelevant articles.
Literature management	Studies retrieved will be exported in Excel format and populated with the agreed information.
Data extraction	The following information will be extracted from each relevant paper by the research team: — Author(s) — Year of study — Title — Country — Types of incidents covered — Type of impact — Research purpose — Key themes covered by research — Research methodology and sources — Limitations (both acknowledge in the study and identified by the team) — Peer reviewed or not — Key findings — Robustness of the methodology — Abstract — Full citation

Appendix 2: Detailed literature review findings

A2.1 Introduction

This Appendix provides a more detailed write up of the findings from the literature review aligned to key research questions posed as part of this study, based on the literature review protocol detailed in Appendix 1.

In total 21 academic studies and 10 sources of grey literature, including Government papers and industry reports, were reviewed. These provide a comprehensive view of the nature of impacts of cyber attacks across CNI. It is noted however, that studies covered by the literature review include examples from a range CNI, and across different countries and scenarios. All findings should therefore be considered indicative, rather than being specific to the scenario under consideration in the study.

A2.2 Literature review findings

A2.2.1 The potential threat and nature of cyber incidents on critical infrastructure

Research question 1: What are the specific impacts if the critical sector is victim to a cyber attack compared to a conventional attack?

In general, the literature reviewed suggests that there are increasing threats of cyber attacks on critical infrastructure. The International Monetary Fund (IMF) reports that the number of cyber attacks has almost doubled since the COVID-19 pandemic.[172] Meanwhile the International Energy Agency (IEA) has stated that cyber attacks on utilities has been growing rapidly since 2018, reaching a peak in 2022 following Russia's invasion of Ukraine.[173]

Over recent years, cyber attacks have become increasingly sophisticated with different configuration types, such as ransomware, malware, manipulation methods, phishing and spear-phishing.[174]

At the same time, technological advancements in and the widespread adoption of information and communication technologies in infrastructures has meant that the threat of cyber attacks is greater and the potential impact more severe.[175] Further, the integration of industrial control systems within CNI and industrial networks means that these systems are increasingly being targeted by malicious actors such as hackers, industrial spies and even foreign armies and intelligence agencies.[176] One study suggests that the greatest threat is from state sponsored cyber attacks as they tend to be more sophisticated and often seek to maximise the level of potential harm that is delivered.[177] The 2015 cyber attack on the Ukrainian power grid and the 2017 WannaCry incident on the NHS are both examples of serious cyber incidents which targeted CNI.[178]

Cyber attacks on CNI offer a particular kind of threat over and above conventional attacks on physical infrastructure. Cyber attacks can easily spread through infrastructure, especially in the age of the industrial internet of things, thereby magnifying the damage compared to what a conventional attack

[172] IMF Monetary and Capital Markets Department (2024) Global Financial Stability Report. The Last Mile: Financial Vulnerabilities and Risks
[173] IEA (2023) Cybersecurity – is the power system lagging behind?
[174] Kendzierskyj, S and Jahankhani, H (2019) The Role of Blockchain in Supporting Critical National Infrastructure, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 208-212.
[175] Kour, R; Karim, R; Thaduri, A (2020) Cybersecurity for railways – A maturity model. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit; 234(10):1129-1148.
[176] Pricop, E; Mihalache, SF, (2015) Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems. 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania.
[177] Kendzierskyj, S and Jahankhani, H (2019) The Role of Blockchain in Supporting Critical National Infrastructure, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 208-212.
[178] Kendzierskyj, S and Jahankhani, H (2019) The Role of Blockchain in Supporting Critical National Infrastructure, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 208-212.

would achieve. Moreover, cyber attacks can be more easily repeated (e.g. attackers coordinating bots to launch several strikes to overwhelm traffic or disrupt a network component), which means that recovery from cyber-related disruptions can take longer to recover from and requires a great deal of coordination from the defenders.

Further, it has been found that for integrated CNI structures, market inefficiencies and a lack of coordination between firms within the structure may mean that there is a greater impact of a cyber incident on one part of the infrastructure. One study suggests the reliance of natural gas pipelines on the generation of electricity as an example of where there may be an additional risk factor from cyber incidents relative to conventional attacks.[179]

In terms of the nature of the impacts of cyber attacks, many of the types of the impacts of cyber attacks will align to the types of impacts from conventional attacks, or wider sources of network disruption. However there are additional potential impacts from cyber attacks specifically. These include financial costs resulting from ransomware or data breaches.[180] Furthermore, the impact of data loss can be substantial if sensitive operational information (e.g. nuclear information, routes, dangerous freight loads etc) is lost.

A2.2.2 Identified impacts of a systemic cyber incident on critical infrastructure

Research question 2: Where are the economic impacts felt across businesses and consumers?

In response to one of the research questions set by DSIT and DCMS at the beginning of this study, the literature review has sought to understand how the impacts of a systemic cyber incident might be felt across businesses and consumers (see Section [X] for more information on the research questions for the study). In the following sections, a summary of the findings from the literature review in relation to the impacts on business and consumers is presented in turn.

Impacts on businesses

The evidence gathered in the systematic literature review suggests that cyber incidents and attacks can increase costs for businesses/organisations targeted through a cyber incident. Studies show that cyber incidents and attacks can generate high costs for targeted business/organisation in the short-term as they may experience shutdowns or equipment failure and may need to repair damaged assets. Further, cyber incidents and attacks can seriously damage the reputation of affected businesses/organisations. Peterman et al. identified that in the case of a cyber attack on the power network, if disruptions are extended over several weeks, the damage can include the public's loss of confidence in the power supply companies or in public authorities.[181]

When CNI is owned by a private business, economic impacts are also felt on targeted businesses' revenues and, in the case of publicly traded companies, stock performance. For example, in September 2024 a cyber attack on Transport for London (TfL) caused some passengers unable to access certain online services. In update to its Board members, TfL stated that the cyber attack had cost the organisation over £30 million (as of December 2024).[182]

A 2018 study on US corporate cyber attacks shows that large firms experienced, on average, a decline in sales of 3.4 percentage points following an attack, with compromised companies in the retail sector experiencing a 5.4 percentage point decline in sales growth. With regards to stock performance when large firms suffered breaches of personal data, such as social security numbers and bank information, the average immediate loss in stock value was 1.12%, or $607 million, based

[179] Carreno, I. L., Scaglione, A., Zlotnik, A., Deka, D., & Sundar, K. (2020) An adversarial model for attack vector vulnerability analysis on power and gas delivery operations. Electric Power Systems Research, 189
[180] James E. Lerums, J. Eric Dietz, (2018). The Economics of Critical Infrastructure Controls Systems' Cyber Security. IEEE International Symposium on Technologies for Homeland Security (HST)
[181] Petermann et al (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage.
[182] Transport for London (2024)

on a mean market value of equity of $54.2 billion. It was found that firms that experienced repeated attacks and/or lacked explicit risk monitoring committees suffer significantly greater losses.[183]

Similarly, the CrowdStrike cyber incident, saw a huge impact on the firm's share price, with a reduction of 22.9% between 18-24 July 2024, representing a change in market cap of around $19 billion.[184] It is noted, however, that the impact on the stock price of CrowdStrike may be particularly high given that CrowdStrike operates in cybersecurity and is not necessarily typical of incidents in other sectors.

It has been found that cyber incidents can have long-run effects on the firms targeted. One study found that the credit ratings of the victims of corporate cyber incidents remain depressed for three years. Further, the firms endure heightened cash flow volatility and report a lower ratio of net worth to total assets.[185]

There is a distinction between the impacts on the businesses that were targeted through cyber incidents and those that experience second-order impacts as a result of the cyber incident. Examples of second-order impacts on businesses from cyber incidents to CNI include:

— Disruption to operations either due to loss of service (e.g. power cuts) or through the upstream supply chain (e.g. as a result of disruptions freight transported via railways).[186] Such disruptions to business operations may result in a loss of revenue for businesses affected.

— A reduction in workforce productivity, for example as a consequence of travel disruption employees unable to travel to work. One study estimated that a cyber incident on the electricity grid in the UK could result in the disruption of more than 800,000 individual train journeys per day in areas affected by the power failure. This could contribute (along with other factors) to a 50% reduction in labour productivity.[187] Another study estimated that a cyber incident to the US electric grid could cause a 10-60% attrition in the workforce across supply chain sectors.[188]

— An impact on the stock value of businesses indirectly impacted by the cyber incident. For example, du the CrowdStrike incident in June 2024, the FTSE 100 closed 0.6% down, equivalent to a reduction of £21 billion in its stock value. In the US, the S&P 500 dropped 0.8%, which is a change in market cap of around $336 billion.[189,190]

Impacts on consumers

In terms of impacts on consumers, the studies reviewed identify that cyber disruptions can affect consumers' productivity, confidence and trust after a prolonged loss of service. One study on major disruptions to the US power grid, for example, highlights that recovery plans in the case of a partial or total shutdown could take up to 5 days, with potential disruption beyond this timescale (Oughton et al. 2017). Similarly, Blouin et al. estimate that a cyber incident severely damaging the US electric grid and leading to a complete loss of electricity would cause a 10–60% attrition of the human workforce across supply chain sectors, and that this attrition would occur within 1–2 days after the onset of the blackout.[191]

[183] Shinichi, et al (2018) What is the impact of successful cyberattacks on target firms?. No. w24409. National Bureau of Economic Research
[184] KOVRR (2024) The UK Cost of the CrowdStrike Incident.
[185] Shinichi, et al (2018) What is the impact of successful cyberattacks on target firms?. No. w24409. National Bureau of Economic Research
[186] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[187] Ibid.
[188] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493.
[189] It is noted that the impact on the stock price of CrowdStrike may be particularly high given that CrowdStrike operates in cybersecurity and is not necessarily typical of incidents in other sectors.
[190] Ibid.
[191] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493

Studies looking specifically at the potential impact of cyber incidents on rail networks identified the following outcomes and impacts for consumers:[192, 193]

- Reduced service levels across the affected parts of the network, leading to a reduction in passenger journeys and/or longer journey times for passengers. Where passengers experience longer journey times or their ability to travel for leisure purposes there may be a loss of welfare. It is noted that studies have experienced difficulty in understanding the degree to which rail services may be impacted by a cyber incident as it depends on the resilience built into the system architecture and the ability for rail operators to switch to a fallback mechanism.
- Loss of goods transported using the freight rail may result in shortages of products.
- Potential loss of life if an attack results in the unsafe movement of trains. Bloomfield et al estimate that in a worst-case scenario, a cyber attack on the UK rail network could result in multiple accidents and collisions on the rail network resulting in multiple injuries and several hundred deaths.
- Loss of public confidence in railway operators, especially if there are repeated cyber incidents leading to a loss of services to the rail network.

Cyber incidents can also negatively impact consumers' disposable income if they reduce the available supply of goods and services such that excess demand puts pressure on prices. A review of the US Colonial Pipeline ransomware attack that occurred in 2021 shows the resulting shutdown led to an average fuel price increase of 4 cents per gallon in affected areas during the rest of the month. Unexpected spikes in fuel prices can impose a strain on disposable household income and reduce overall spending on other goods and services, thus slowing economic growth.[194] This may particularly be the case for essential goods such as fuel, where temporary reductions in consumption of the effected goods, and substitution to other goods, may not be possible.

The impact of cyber attacks on UK critical infrastructure is also documented in analysis of real-world scenarios. A review of the impact of the Wannacry incident on the NHS showed that incident resulted in an outage of the EMIS Health system.[195] This outage prevented many GPs from being able to digitally manage appointment bookings and patient records and send prescriptions to pharmacies. GPs also reported having to delay urgent tasks such as writing referral letters for patients with suspected cancers.[196] Northern Ireland was also impacted by the Wannacry incident, where 75% of GPs use the EMIS Health system and had to delay suspected cancer referrals.[197]

Impacts on the economy

Studies have also identified potential impacts of systemic cyber incidents on the wider economy.

To the extent that a cyber incident impacts businesses and consumers, this can feed through into wider impacts on a country's economy. This would be more likely in the case of a systemic cyber incident given the expected far-reaching nature of these incidents. Evidence collected through the literature review suggests that one of the key economic impacts of cyber incidents is a loss of productivity and output as business operations for both the business affected and those in the downstream supply chain are disrupted. Ultimately, studies show that this can have a real impact on a country's Gross Domestic Product (GDP).

The complexity of the supply chains in which critical infrastructures are embedded can lead to cascading effects on other sectors of the economy.[198] For example, one study modelled the potential

[192] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science
[193] Reitšpís, J., & Mašľan, M. (2021). Possibilities of prevention and reduction of threats affecting the safety and fluidity of land transport. Baltic Journal of Economic Studies, 7(4), 18-23.
[194] T. Tsvetanov, S. Slaria. (2021) The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters Volume 209, December 2021, 110122
[195] The EMIS Health system supplies electronic patient record systems and software used in the NHS.
[196] Ghafur et al (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digit. Med.* 2, 98 (2019).
[197] Ghafur et al (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digit. Med.* 2, 98 (2019).
[198] Tam et al (2023) Quantifying the econometric loss of a cyber-physical attack on a seaport. Front. Comput. Sci., 23 January 2023 Sec. Computer Security Volume 4 - 2022

impact on the economy of an attack to the UK power grid in the South and East regions of the UK is estimated to potentially disrupt 40%-55% of UK port freight. The attack would be expected to impact Felixstowe, the main container port in the UK, and Dover, which is strategically important for supply chain distribution to and from Europe, with impacts felt by businesses and consumers as deliveries would be unable to get to their destination. Shortages of food and petrol would cause further economic damage as well as social stress. Exports and imports could decline in direct proportion to the volume of cargo going through Dover, Felixstowe and London for the duration of the electricity outage, whilst sectors like domestic and air travel, road transport, and tourism could also be hampered.[199]

Another study modelling a 5-week cyber incident on crude oil terminals in the Gulf of Mexico estimates that the scenario could result in 80% reduction in crude oil availability for Gulf-area refineries and a 40% reduction in U.S. crude oil availability for the affected time period.[200]

Another study focused on Germany estimates that, in just 2 hours, an unexpected and widespread power blackout could lead to severe disruptions in urban areas, as traffic lights, traffic management systems and road lighting stop working, which can lead to a rise in traffic accidents and risks to public safety. A lack of electricity would prevent vehicles from filling up at petrol stations, whilst passenger and goods traffic on the rail network would be disrupted. Overall, there would be a considerable slowdown in shipping into and out of ports, whilst delays in shipping goods could cause financial damage to firms.[201]

Further, the global nature of present-day supply chains means that the impacts of cyber attacks may not be contained to the country targeted but may have international implications.[202]

The scale of the impact of a cyber incident to CNI can also be driven by the market concentration of the sector. When there is a higher concentration of firms owning and operating CNI, a cyber incident could have a greater impact on the economy as many more firms in the downstream supply chain will be connected.[203]

A2.2.3 Estimated economic costs of a systemic cyber incident

Research question 3: What are the economic costs of the attack? This includes both direct (e.g. immediate financial losses and recovery costs); and indirect costs (e.g. those resulting from reduced investments; and reduced consumer confidence in the sector).

There is limited evidence from existing literature on the potential economic costs of systemic on the rail network. It is noted in studies that it is difficult to estimate the economic costs of a cyber incident to the rail network as there is insufficient public information on the extent to which a cyber incident might disrupt the operations of rail services.[204] The scale of disruption to rail services and the second-order impacts on freight operations and people's ability to travel to work will be the key drivers to estimating the economic cost of cyber incident on the rail network.

However, evidence from cyber incidents on other forms of CNI show that cyber disruptions can have economic effects in terms of inoperability and damage to specific sectors of the economy, which in turn impact GDP.

Cyber disruptions can have concrete economic effects in terms of inoperability and damage to specific sectors of the economy, which have an impact on GDP. For example, Kelly et al. estimate that a power blackout in the UK due to a cyber incident lasting between 3 and 12 weeks would

[199] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[200] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[201] Petermann et al (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage.
[202] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[203] KOVRR (2024) The UK Cost of the CrowdStrike Incident.
[204] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science

produce economic losses in the range of £11.6 billion to £85.5 billion depending on the length of recovery. Analysis of the combined direct and indirect impact by sector shows that Financial Services would be particularly affected with a total loss of £1.3 billion, whilst other affected critical infrastructure sectors would include Health (£0.7 billion), Transport (£0.6 billion) and Government and Emergency Services (£0.5 billion). Other affected services include Wholesale and Retail Trade (£1.3 billion), Real Estate Activities (£1.2 billion), Professional Services (£1 billion), and Construction (£0.8 billion).[205]

With regards to GDP, in the same study the authors estimate that the overall GDP impact of the attack would amount to a loss of between £49 billion to £442 billion across the entire UK economy in the five years following the outage when compared against baseline estimates for economic growth.[206] Another study modelling the impact of a 5-day cyber disruption on the electricity distribution network serving London and the South East of England estimates GDP loss ranging from £20.6 million up to £111.4 million.[207, 208] Whilst both of the studies set out above estimates relate to large scale attacks, the literature shows that shorter disruptions can still result in substantial economic damage. For example, it is estimated that a 1-hour power disruption on a working day in winter in a country like Germany would result in economic damage between EUR 0.6 billion and EUR 1.3 billion at the overall economy level.[209]

Due to economic interdependencies, impacts on the UK economy are documented even in the case of distant attacks. A 5-day disruption on a major European port like Valencia could have cascading effects on countries like the UK, with a loss of £1.3 billion measured in terms of companies' lost market shares and revenue.[210] Similarly, a study measuring the impact of the recent CrowdStrike outage in the US, which caused disruptions for 24 hours, has calculated that the total cost to the UK economy falls between £1.7 and £2.3 billion.[211]

Studies show evidence of both substantial direct and indirect costs due to cyber disruptions to critical infrastructures. For instance, the total cost (capturing the disruption loss and recovery loss) of a hypothetical cyber incident disrupting crude oil supply in the US Gulf Coast area is estimated to amount to USD 8 billion, including disruptions in regions like the East Coast, Midwest, Rockies, West Coast, and Gulf Coast.[212]

Indirect costs are also documented in detail. Oughton et al measure lost investment the UK economy ranging from £6 to £34 million in the year the incident takes place in the scenario of a cyber-physical attack disrupting the electricity network in London, whilst lost capital stock formation is estimated to range from £12 to 74 million in the year following the incident.[213]

Indirect costs are also measured in terms of service interruption for consumers and cascading effects on other sectors like water, transport, telecoms and waste.[214] A major disruption to the UK power network in the South and East region lasting several weeks is estimated to potentially produce a total lost GVA of £11.6 billion. The modelling of this scenario suggests that for every £1 lost directly in the cyber attack, roughly £0.62 is lost directly and £0.38 is lost indirectly in commercial production activities.

Finally, some studies include loss of life as a potential consequence of cyber-physical attacks to critical sectors of the economy. For instance, it is estimated that an attack to the rail network causing

[205] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[206] Ibid.
[207] Based on between 4 and 14 substations impacted.
[208] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[209] Petermann et al (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage.
[210] Tam et al (2023) Quantifying the econometric loss of a cyber-physical attack on a seaport. Front. Comput. Sci., 23 January 2023 Sec. Computer Security Volume 4 - 2022
[211] KOVRR (2024) The UK Cost of the CrowdStrike Incident.
[212] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[213] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[214] Ibid.

"unsafe movement" of a convoy could cause an accident with 100 or more deaths in the worst-case scenario.[215]

6.4.1 Methodologies used to model the economic costs of systemic cyber incidents

Research question 4: What is the best methodology to model such an attack?

The literature review identified a number of commonly used methods to model the economic costs of systemic cyber incidents applied in existing literature.

Most studies are based on economic modelling and other related econometric analyses. Studies often rely on inoperability Input-Output models - computer-based models that analyse the impacts created by disruptions on the interactive operations of economic and infrastructure sectors. These models can also identify the distribution of direct and indirect impacts of an attack across sectors.[216, 217] These have the benefit of being replicable, generalisable and scalable, but lack the specificity of bespoke analysis based on behavioural response and wider context and broader, difficult to quantify impacts.

To account for qualitative factors of a specific scenario, some studies triangulate quantitative modelling with structured interviews with stakeholders and representatives of critical industries, government, and regulatory agencies.[218] To better account for the possibility of various outcomes under uncertainty, some studies model the potential impact of different scenario using counterfactual analysis.[219, 220, 221] In the case of Oughton et al, the study utilises both upward and downward counterfactual scenarios. Downward means considering what would have been the damage if a greater number of stations had been impacted, while upward investigates the damage in the case of fewer substations being attacked. [222] These have the benefit of being able to take into account specific impacts based on the context of the attack and capturing harder to quantify impacts, but are more resource intensive to implement due to the requirement for primary research (e.g. interviews with a large range of informed stakeholders).

Where data and evidence allow, studies often deploy system-dynamics models or sectoral analyses to simulate how consumers are affected by disruptions like price hikes, internet shutdowns, and transport failure as a result of attacks on critical infrastructures.[223, 224, 225, 226] In some cases, studies test the plausibility of the developed models or scenarios against past incidents occurred in other countries where there is sufficient real-world data to be able to apply the scenario to a hypothetical

[215] Bloomfield et al (2016) The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science
[216] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[217] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[218] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[219] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[220] Joost et al (2007) A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies. Risk Analysis, Vol. 27, No. 5, 2007.
[221] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[222] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[223] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493.
[224] Kelly et al (2016) Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
[225] T. Tsvetanov, S. Slaria. (2021) The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters Volume 209, December 2021, 110122
[226] Petermann et al (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage

study.[227, 228] These have the benefit of offering the most comprehensive and insightful modelling, providing a much richer picture of the integrated financial and non-fungible costs of an attack. However, the requisite data is difficult and expensive to acquire and the analysis takes time. Furthermore, these types of studies tend to be very bespoke, which can limit their generalisability.

Finally, some studies assess the impacts of past attacks on critical infrastructures.[229] One example of this is a retrospective analysis of the impact of the Wannacry incident on the NHS, which uses data from Hospital Episodes Statistics (HES) to determine the number of cancelled outpatient appointments, the impact on emergency and elective admissions, the number of accident and emergency (A&E) attendances, deaths, and the financial impact on activity. The usage of real-world data is less common as there are inherent difficulties in gathering data about cyber disruptions to critical infrastructure and it relies on organisations being transparent about any cyber incidents and the severity of these. While potentially allowing for detailed study of the impact of a specific attack, the findings from this approach are very bespoke and may not be generalisable to other attacks.

[227] Blouin et al (2024) Assessing the Impact of Catastrophic Electricity Loss on the Food Supply Chain. International Journal of Disaster Risk Science (2024) 15:481–493.
[228] Oughton et al (2019) Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks
[229] Sullivan, Julia E., and Dmitriy Kamensky (2017) How cyber-attacks in Ukraine show the vulnerability of the US power grid The Electricity Journal 30.3 (2017): 30-35.

www.kpmg.com/uk