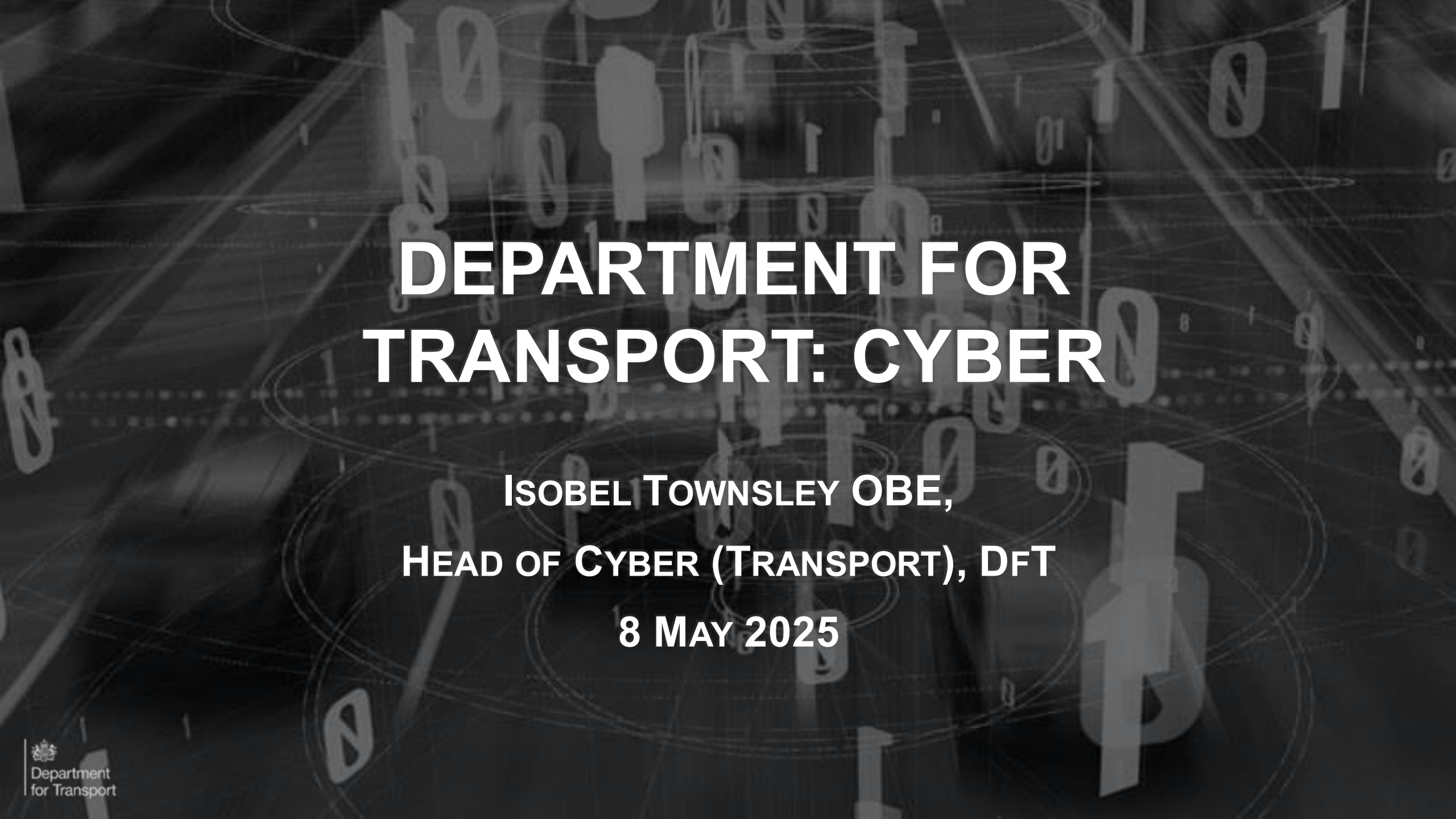


DEPARTMENT FOR TRANSPORT: CYBER

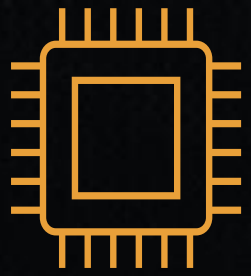
ISOBEL TOWNSLEY OBE,

HEAD OF CYBER (TRANSPORT), DFT

8 MAY 2025

Department for Transport

AGENDA



Cyber as a threat to Transport

How DFT approaches cyber

Overview of challenges

Department for Transport

Jaguar Land Rover Allegedly Hacked – Threat Actor Leaked 700 Internal Documents

Split Airport hacked by Akira ransomware gang

TfL cyber attack: What you need to know

UK rail network Merseyrail likely hit by Lockbit ransomware

Volkswagen Data Breach: 800,000 Electric Car Owners' Data Leaked

Major UK transport company Go-Ahead battles cyber-attack

Firm says software used to schedule bus services hit but Thameslink rail operations not affected

"It's not just CrowdStrike - the cyber sector is vulnerable"

Train station Wi-Fi cyber attack: London's biggest hubs including King's Cross and Waterloo hit by 'Islamophobic cyber attack'

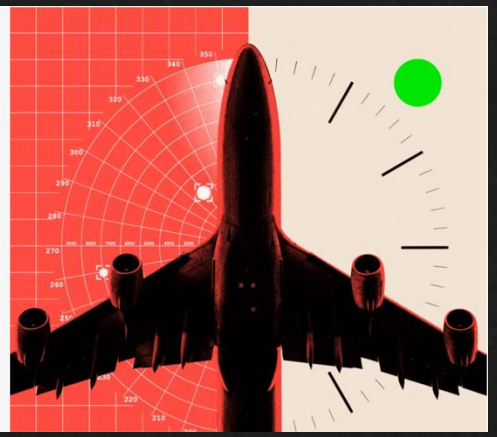
Cyberattack Disrupts Japan Airlines Operations, Delays Over 40 Flights

DP World hack: port operator gradually restarting operations around Australia after cyber-attack

BBC INDEPTH

Planes are having their GPS hacked. Could new clocks keep them safe?

3 March 2025



LIVE: Manchester Airport website goes down as Russian 'hackers' claim responsibility

MOVEit hack: BBC, BA and Boots among cyber attack victims

Department for Transport

Actor	Motivation	Standard Methodology
 State Actor	Gathering intelligence disrupting critical infrastructure, stealing intellectual property, and undermining geopolitical rivals.	Highly skilled and well-funded – zero-day exploits, supply chain attacks, sophisticated social engineering tactics
 Criminal	Potential for monetary reward.	Phishing attacks, ransomware, malware, identity theft
 Terrorists	Spreading propaganda, disrupting critical infrastructure, and instilling fear through cyberattacks.	Cyber attacks that cause physical harm or disrupt public services.
 Script Kiddies	Boredom, curiosity, desire for notoriety in the hacking community.	Low-sophistication attacks including targeting unpatched systems and weak passwords. Cyber-attack as a service purchases.
 Hacktivists	Promote political, social, or ideological causes.	Defacing websites, DDoS attacks, leaking sensitive information.
 Insider Threat	Financial gain, revenge, ideological reasons.	Use legitimate access to systems for data theft, sabotage, or unintentional breaches due to negligence.

CYBER IN DFT

DfT Digital Information Services & DfT Corporate Security Teams

Responsible for the cyber security of DfTc and DfT ALBS (incl. regarding DfT data security).

Use GovAssure

NSD Cyber Team

Acts as a central cyber team for DfT, focus is cyber security of transport sector (road, rail, maritime & aviation).

Acts as both policy lead and Regulator including for some DfT ALB transport operators.

Enforces the Network & Information Systems Regulations 2018 (NIS) for road, rail and maritime

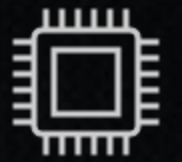
DfT modal resilience teams

Road, Rail, Maritime & Aviation

Support cyber team (and vice versa) by delivering modal resilience policy, including cyber e.g. guidance, specific changes to modal legislation, broader engagement

Department for Transport

NSD CYBER TEAM



PROGRAMME: Understanding threats & vulnerabilities, Horizon scanning (threat & tech), programme management

THREAT & RISK: Cyber Methodologies, Emerging Tech – AI, Quantum, Risk (Modal, cross sector)

REGULATORY POLICY: New/Amending Regulations (Policy development), Supply Chains

EXERCISING & INCIDENT MANAGEMENT: DfT Response, Exercising: Internal & External (cross sector), Industry Comms (crisis, alerts)

REGULATORY COMPLIANCE (CYBER): Enforces NIS (2018) Regulations, regulatory guidance

Department for Transport

CYBER COMPLIANCE

Network & Information Systems (NIS) Regulations 2018

Designates Operators of Essential Services (OES) within Transport.

Applies thresholds for level of impact of a cyber event on transport services affected (passenger numbers, freight tonnage etc.).

Impact based so less focused on cause – e.g. malicious cyber, non malicious cyber, non-cyber included under NIS.

NSD Cyber

Competent Authority for Road, Rail, Maritime & Aviation (co-competent authority for aviation with Civil Aviation Authority) under NIS.

Assess OES compliance with NIS Regulations using the NCSC Cyber Assessment Framework (CAF).

Provide OES with clear guidance to help them meet the requirements of the NIS Regulations.

Ensure processes are in place for notifications of NIS incidents and (if required) post-incident investigation.

NIS Regulated Entities

AVIATION – 13 OES

RAIL – 45 OES

ROAD – 2 OES

MARITIME – 9 OES

Assurance across 250+ critical transport systems.

CYBER CHALLENGES

Poor risk understanding

Variable levels of cyber maturity across transport and within each mode

Supply chain vulnerabilities

Continued Investment

Legacy Systems

Emerging tech: increasing use of AI, Quantum

Department for Transport

Department
for Transport