Cyber Risk and Threat Quarterly

Department for Transport — September 2026

Accessible text version of the original slide-based newsletter. Decorative images have been omitted; diagrams and infographics have been converted into plain text below.

Useful Links

- Cyber Essentials
- Active Cyber Defence services
- Mitigating malware and ransomware attacks
- National Protective Security Authority | SeCuRE
- Sign up link - NCSC Early Warning System

Recent update: Follow the NCSC's latest guidance on internet-exposed systems and edge devices (see NCSC.GOV.UK). Any organisation that uses, deploys or maintains OT systems should read the guidance and review their security posture accordingly.

Reporting cyber incidents (transport organisations):

- cyber@dft.gov.uk (non-NIS)
- NISIncidents@dft.gov.uk (NIS only)

Cyber Preparedness

Cyber threats continue to evolve, making preparedness an essential component of organisational resilience. While organisations invest significant effort in preventing incidents, it is equally important to ensure they can respond effectively when an incident occurs.

Developing robust response arrangements, regularly exercising plans, and embedding lessons learned can help reduce the impact of cyber incidents and improve recovery outcomes.

Incident Response Plans: What are they?

An Incident Response Plan provides a structured approach to managing cyber incidents, helping organisations respond quickly, coordinate effectively, and recover efficiently while minimising disruption.

What should they contain?

- Key contacts
- Escalation criteria
- Roles and responsibilities
- Legal or regulatory requirements
- Checklists/templates

- Crisis crates and business continuity
- Playbooks

Key Stages of Incident Response Plans

These foundations provide clarity on roles and responsibilities, support effective triage and escalation, and help ensure incidents are managed consistently. They also enable organisations to capture lessons identified and improve future incident management.

Exercising Incident Response Plans

Regularly exercising your Incident Response Plan helps identify gaps before incidents occur, build confidence in response and recovery arrangements, and validate that plans, processes and people can work together effectively under realistic conditions.

How to Report an Incident

Transport organisations can report cyber incidents to the Department for Transport at:

- cyber@dft.gov.uk (non-NIS)
- NISIncidents@dft.gov.uk (NIS only)

What to Do When Something Happens

This process is described below as a decision flow, starting from when a cyber incident is identified.

Step 1: Cyber incident identified.
Step 2: Does the incident meet mandatory thresholds set out under NIS (the Network and Information Systems Regulations)?

If Yes — mandatory reporting under NIS regulations:

1. Mandatory reporting: NIS regulations.
2. Notify the regulator and relevant authorities.
3. Report to DfT via NISIncidents@dft.gov.uk and NCSC.

If No — proactive reporting is still encouraged by DfT (for both OES and non-OES organisations):

1. Proactive reporting encouraged by DfT (OES and non-OES).
2. Contact NCSC and email DfT at cyber@dft.gov.uk.
3. Out of hours? Report via TSOC at TSOC@dft.gov.uk.

Note: *you may find you follow both pathways! Many NIS incidents begin as proactive reports, allowing DfT to provide early intervention.*

Incident Case Study: Recruitment Impersonation Attempt

The following timeline sets out how a recruitment impersonation scam unfolded and was handled, in six stages.

1. Initial Contact

An organisation identified suspicious emails impersonating a member of its HR team. Recipients were contacted about a purported job opportunity and encouraged to engage in further correspondence.

2. Trust Established Through Recruitment Scheme

The approach used a legitimate-looking recruitment scenario to build credibility and begin a dialogue with recipients, increasing the likelihood of engagement.

3. Potential Delivery of Malicious Content

The recruitment conversation was likely intended to progress to the sharing of malicious files disguised as job descriptions or other recruitment documentation.

4. Suspicious Activity Reported

The fraudulent approach was identified and reported by the affected organisation before any compromise was confirmed, enabling early investigation and response.

5. Threat Intelligence Shared

Details of the scam were circulated to relevant sector partners to raise awareness, support detection activity and help organisations identify similar approaches within their own environments.

6. Mitigation Actions Implemented

Organisations were advised to block the malicious sender, search for related emails within their mail systems, remove any identified messages, and report suspected compromise through established cyber incident reporting channels.

What Is Legacy Technology?

The DfT has been looking at the subject of legacy technology and its implications for the cyber security of the transport sector. Legacy technology is not defined by age alone. Technology becomes "legacy" when it becomes difficult to maintain, secure, integrate or change safely. These technologies can increase cyber security risk by limiting an organisation's ability to implement security updates, integrate new capabilities and respond effectively to evolving threats.

These challenges are particularly important in transport environments, where systems can have long operational lifecycles, support critical services and depend on a wide range of other technologies, suppliers and organisations.

Key Pressures

The most significant pressures identified were:

- Operational impact
- Security risk
- Integration complexity

Key Findings

1. Cyber risk often concentrates at the connections between systems, rather than within individual technologies alone. Systems that enable information or services to pass between different operational domains can carry several pressures at once. Weaknesses at these interfaces may therefore affect multiple systems or organisations, making clear ownership, coordination and ongoing assurance particularly important.
2. Modern technology can develop legacy characteristics if it becomes difficult to update, is tightly integrated or relies on outdated protocols and security standards.

Managing the Risk

Legacy technology risk is not only about replacing older assets. Effective management requires organisations to:

1. Understand critical dependencies.
2. Strengthen security at system boundaries.
3. Maintain effective identity and access controls.
4. Continuously review risk.
5. Ensure future systems are designed and procured with clear upgrade pathways and the ability to adapt over time.