Cyber Risk and Threat Quarterly

Department for Transport

"Cyber risk is no longer just an IT issue — it's a boardroom priority."
NCSC Annual Review 2025

Useful links:

Cyber Essentials - NCSC.GOV.UK

Active Cyber Defence services - NCSC.GOV.UK

Mitigating malware and ransomware attacks - NCSC.GOV.UK

National Protective Security Authority | SeCuRE

Sign up link - NCSC Early Warning System

Transport organisations can report cyber incidents to the Department for Transport at: cyber@dft.gov.uk (non-NIS) NISIncidents@dft.gov.uk (NIS only)

Middle East Conflict ⚠

In light of recent events in the Middle East, the NCSC has issued a public alert with an update on the current threat landscape and recommended actions for organisations. We encourage readers to review the alert here: Alert: NCSC advises UK organisations to take action

If you have any concerns, you can report these using the NCSC's Report a Cyber Incident tool.

Welcome to the first issue of DfT's Cyber Risk and Threat Quarterly. This first edition focuses on incident response, attacker behaviours, and recent regulatory updates, with future editions shaped by the evolving threat landscape.

What to do if you are hacked:

When cyber attacks occur or services are disrupted, NCSC provide incident response to minimise harm, restore operations. The respond and recover advice from NCSC will help transport organisations back on their feet if they have suffered an attack.
Organisations can find out where to report a cyber incident in the UK using the signposting service at Where To Report A Cyber Incident .

NCSC Annual Review 2025: Key Takeaways for Transport

Ransomware – Remains a top threat to critical infrastructure and essential services.

State-Linked Threats – Nation-states and advanced criminal groups target transport and logistics.

Supply Chain – Weaknesses in suppliers and third-party systems must be addressed.

Tools and Guidance – Cyber Action Toolkit and CAF v4 help manage cyber risks.

Cryptography & Emerging Tech – Focus on secure-by-design, next-gen cryptography, and AI risk management.

March 2026

Cyber Risk and Threat Quarterly

Department for Transport

Trends in tactics, techniques and procedures (TTPs):

Finding weak links in supply chains

Hackers can find software partners, which they know their victim will trust and rely on. An attack will then leverage zero-day flaws in software or hardware to gain undetected access to the partner's network and create a hard-to-detect route into the main target's secure systems, to deploy ransomware.

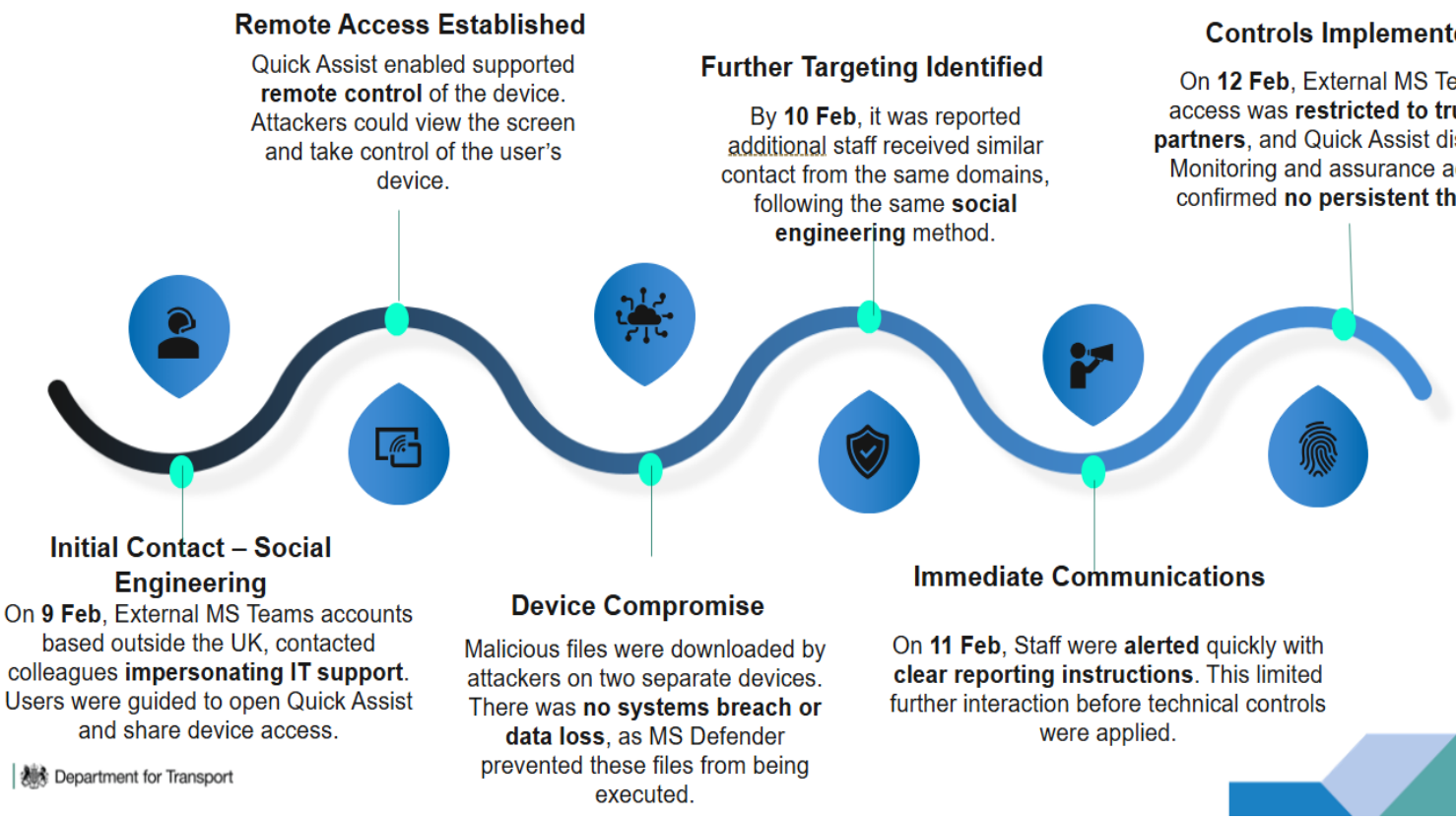
Wireless Access Exploitation and Signal Spoofing

Flipper Zero is a pocket-sized multi-tool that reads and emulates common access technologies (RFID/NFC, sub-1GHz, IR, BLE, USB), used by hobbyists and penetration testers. They are sold on underground markets and can be used to intercept or clone key-fob signals and unlock various car models, prompting industry warnings.

Helpdesk Tactics:

One common tactic involves overwhelming an employee with phishing emails, then calling them while posing as the help desk to "resolve" the issue. Another method sees criminals impersonating employees when contacting the help desk, persuading staff to reset passwords or disable multi-factor authentication.

Reported MS Teams Impersonation Attack (sharing for awareness)



NCSC Phishing Guidance

March 2026

Cyber Risk and Threat Quarterly

Department for Transport

Regulation: Cyber Assessment Framework v4.0 Updates

1. Attacker Intelligence (A2.b)
Stronger emphasis on using real-world threat intelligence. Operators should track current attacker behaviour (e.g., ransomware, logistics disruption) and use it to guide risk decisions and incident preparedness.

2. Secure and Supported Software (A4.b)
New focus on ensuring all software underpinning essential services is secure and supported. Know what you use, plan to remove or mitigate unsupported components, and obtain assurance from suppliers on testing, patching, and version control.

3. Proactive Threat Detection (C1 & C2)
Higher expectations for monitoring and a new requirement for threat hunting. Move beyond passive alerting to actively look for signs of compromise- such as unusual traffic or authentication anomalies—using internal teams or managed services.

4. AI and Emerging Technology Risks (A2 & B4)
AI-related risks are now embedded across CAF outcomes. Identify where AI is deployed, assess associated risks, and ensure systems are secure by design with validated inputs, controlled interfaces, and clear recovery processes.

For more information on the CAF, contact: *cybercomplianceteam@dft.gov.uk*

Cyber Security and Resilience Bill

On November 12th, the Government introduced The Cyber Security and Resilience (Network and Information Systems) Bill to the House of Commons. The Bill aims to strengthen UK cyber defences by updating the existing regulatory framework. Key measures include expanding scope to cover critical suppliers, enhancing regulatory powers, and enabling future resilience.

Cyber attacks are increasingly affecting organisations both directly and indirectly via their supply chains, highlighting vulnerabilities across interconnected systems. For instance, in August 2024, Transport for London suffered a cyber incident that affected various IT services while in September 2025, Collins Aerospace, a key aviation supplier, was targeted, resulting in downstream impact. In response to these evolving threats, and as co-regulators for the transport sector, the DfT and the Civil Aviation Authority have launched a mapping programme to identify which critical suppliers may fall within the Bill's proposed regulatory scope.

For more information on any of the topics covered in the newsletter, please contact **cyber@dft.gov.uk**