Cyber security at the GLA

padlock on keyboard

Key information

Publication type: General

Publication status: Adopted

Publication date: Thursday 12 February 2026

S

The Transport for London (TfL) cyber-attack in September 2024 took place just as the **GLA Oversight Committee** launched its investigation into cyber security at the Greater London Authority (GLA), giving real-time experience of the threat and the work required to mitigate it. While information remains limited even a year after that attack, in part due to ongoing criminal cases, this report sets out what information is publicly available about the attack and how it impacted the GLA, which shares some of TfL's IT systems.

The **GLA Oversight Committee** has published a report on Cybersecurity which makes a number of recommendations, including:

- The GLA and its functional bodies should develop an approach to measuring and monitoring its cyber security investment and pay, and how this can be benchmarked with others in the public and private sector.
- The GLA should use its chairmanship of the London Resilience Forum (LRF) to maintain a proportionate focus on cyber resilience in London, developing expertise and agreement on how the LRF and constituent organisations would respond to a successful major cyber incident in London.
- The GLA should confirm that the GLA has tested and proven plans and contingency arrangements in the event of a cyber incident that prevents staff from accessing their emails and files.
- By the end of this 2025-26 financial year, the GLA should work with TfL to run its own cyber security exercise considering the response to an attack targeting the GLA.

[Read the report in full](#)