

Cybersecurity

Key information

Publication type: Current investigation

Publication status: Adopted

Contents

[Introduction](#)

[Investigation aims and objectives \(Terms of Reference\)](#)

[Key issues](#)

[Key questions](#)

Introduction

The GLA Oversight Committee is investigating cybersecurity, following a rising trend of reported cyber incidents.

Investigation aims and objectives (Terms of Reference)

- To identify areas of weakness of public sector organisations against cyber incidents and to identify any emerging issues and potential solutions in this area.
- To scrutinise the effectiveness of the GLA Group's cyber security processes and benchmark against industry good practice.
- Beyond the technical issues, to understand what cultural lessons need to be learned to keep data and systems safe at the GLA.

Key issues

- As public sector organisations become increasingly dependent on data, computer systems and services, they become subject to a growing variety of increasingly sophisticated security threats, including viruses, hackers and computer-assisted fraud. Cyber attacks affecting public bodies like the NHS, Electoral Commission and local councils have made headlines for the disruption to public services and the sensitive data that they have breached.

- The GLA Group, being a public sector organisation, is also subject a growing variety of increasingly sophisticated security threats. The GLA, being a government institution, also faces risks from politically motivated attacks by agents acting on behalf of foreign states.
- Security experts have raised concerns about the vulnerability of public sector IT infrastructure at a time when hacking by state-backed foreign actors is on the rise. Given the landscape of increasing threat of ransomware attacks, the GLA needs to be appropriately equipped to mitigate these threats.

Key questions

- What are the reasons behind the various cyber attacks against public sector organisations in the past few being successful?
- What lessons have been learned from these recent large-scale attacks? Are they being implemented successfully?
- Are the main barriers to successful cyber security strategies technical or cultural?
- What are the biggest cyber security threats currently facing public sector organisations? Does the GLA have the appropriate resources and crisis management plans in place to mitigate these risks?
- What would the consequences of a cyber attack on the GLA Group be for London?

[Back to table of contents](#)