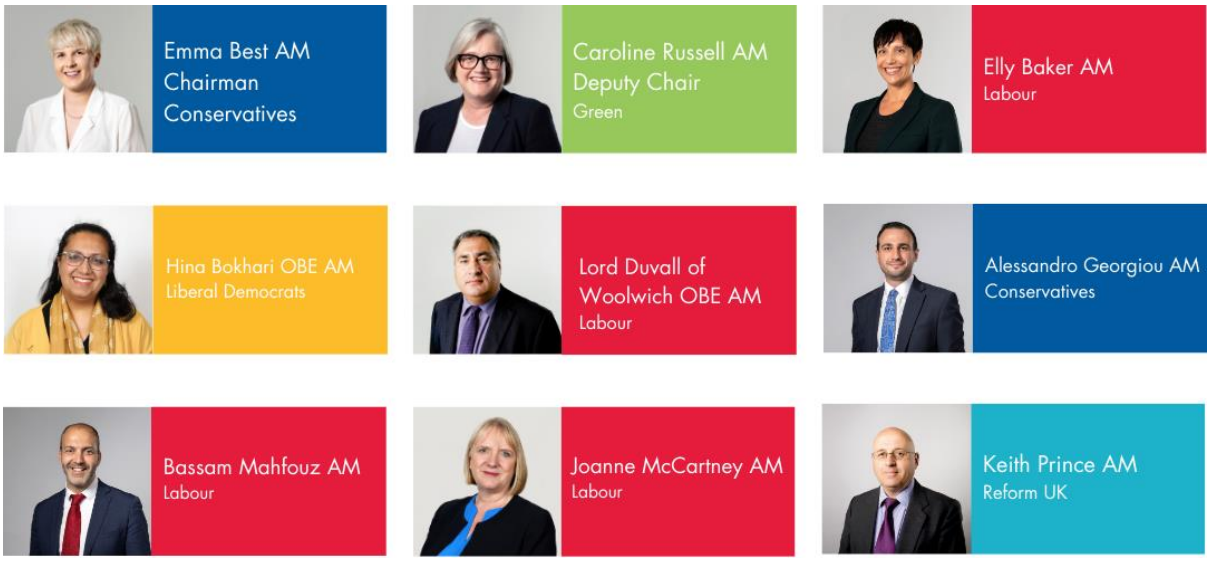
Cyber security at the GLA

GLA Oversight Committee

February 2026

LONDONASSEMBLY

GLA Oversight Committee



The GLA Oversight Committee monitors scrutiny expenditure and oversees the programming of the Assembly's business. It also recommends to the Mayor a budget proposal for the Assembly and allocates the budget for the financial year.

This investigation was carried out by the Oversight Committee in 2024-25, with Emma Best as Chairman, and the Assembly Members listed above.

Contact us

Zoë Oliver-Watts
Assistant Director
Zoe.Oliver-Watts@london.gov.uk

Alison Bell
Head of Assembly Communications
Alison.Bell@london.gov.uk

Judith Smyth
Principal Committee Manager
Judith.Smyth@london.gov.uk

Contents

Foreword

Emma Best AM
Chairman of the GLA Oversight Committee 2024-25

We launched this investigation into Cyber Security at the GLA in 2024 in response to the ever-growing sophistication and damage of cyber-attacks within the public sector. With the nature of these attacks changing so drastically we also wanted to raise awareness of just how impactful they are, not just in the virtual world but also in the physical one.

A week before our first formal meeting TfL suffered from its biggest cyber-attack in history with critical impacts across the system. It also affected the GLA which was part-way through a shared services transition onto TfL's digital platforms. This attack underlined the importance of our investigation and need to review our defences.

During the investigation we were able to hear from the TfL and GLA leaders responsible for our cyber-defence, and review their readiness approach. I'd like to reiterate our thanks to all those in TfL and the GLA who worked on the cyber-attack and its recovery.

The TfL attack caused headlines and shocked the nation when two teenagers were arrested and charged with being involved in the hacking attack. Since then there have been more worldwide incidents garnering media attention as well as further film and drama series portraying of some of the real life impacts of large scale cyber-attacks. Both authorities and the public are recognising the scale of the future risk, especially coupled with the speed of acceleration of AI technology.

For Londoners, we seek further assurance from that the GLA and its associated bodies that everything possible is being done to defend against the next attack. In that context, this report makes eleven recommendations intended to strengthen the GLA's approach to cyber security here in London.

Executive Summary

Today's public sector organisations face a constant threat of cyber attacks. In the online world, the collected personal data of citizens is valuable, and whole organisations' operations can be brought to a halt in order to extract a ransom. Local government is a particular target, reporting three to four times more cyber incidents than national government. In many ways, we are less secure now than we were 50 years ago. Recent cyber attacks on public sector bodies in London such as the British Library, NHS Synnovis and Hackney Council have paralysed those institutions – suspending normal operations for months and costing millions to recover.

As London's strategic authority, it is critical that the GLA grasps the scale of the cyber threat in London, and takes active steps to mitigate it. We set out to examine the risk to public sector organisations like the GLA in London, and to understand how the GLA is managing this risk.

Cost is a major factor, and we heard about the difficulty for public sector organisations in competing with the salaries and investment of the private cyber security sector. Given that the consequences of under-investment can be grievous, we were surprised by how difficult it was to ascertain how much the GLA was investing, and how this compared with others. The GLA must find a way of benchmarking its level of spending on cyber security in order to determine the correct range.

We also considered key actions taken by public sector bodies to prevent attacks, and the challenges to implementing them. Legacy systems are often blamed for creating vulnerabilities, as are complex supply chains. Both may have a place in the public sector in the context of financial constraints, but the dangers must be clearly understood in order for leadership to make informed decisions about risk. We recommend that confidential reporting on these specific vulnerabilities is done on a regular basis.

The importance of a strong cyber security culture was highlighted throughout the investigation, reflecting the fact all individual colleagues could be subject to phishing and other forms of cyber attacks, and must be informed and aware of the dangers. As the GLA looks to build its cyber security culture, it should not ignore the reality of the broader IT culture in the organisation, and the pressures upon it as a result of the IT Shared Services transition to the TfL platform.

Given the inevitability of further cyber attacks, cyber security must also be a key focus for the senior leadership team in the GLA, and a visible and habitual part of its governance structures. The risk appears to have been well-prioritised at TfL, which had run a full cyber security exercise before it experienced the cyber incident in 2024. The GLA's prioritisation of cyber security increased markedly in the wake of the incident, placing it first on the risk register, for the first time. We are satisfied that cyber security is now high on the agenda for corporate teams across the GLA and TfL - how could it be otherwise, given the profile of the TfL cyber incident in 2024. We welcome this awareness and focus, and would now like to see GLA senior management adopting a fluency and maturity in their approach to cyber security issues.

Resilience to a cyber incident is also a critical concern. A cyber attack that restricted the GLA's access to main systems of email, teams documents and shared drives would significantly limit the ability of the majority of staff to do core tasks. The GLA does not provide key services as

councils do, so the impact on the public would be less immediate, but the impact of such a withdrawal of access on the business operations of the organisation would be profound. We would welcome assurance to this Committee, and all GLA staff, that the senior leadership has in place tested and proven plans and contingency arrangements. This would also help demonstrate and bolster the organisational culture of cyber security that has been recognised as a key part of our defence.

The GLA's responsibilities relating to cyber risk and resilience go beyond its operation as an organisation. As a Category 1 responder under the Civil Contingencies Act, and leader of the London Resilience Group, the Mayor has significant responsibility for cybersecurity across all of London's public sector. The London Resilience Forum (LRF) has prioritised cyber security in discussion in 2025. We welcome this approach and necessary prioritisation at this high level forum of cyber risk and resilience, which is more than likely to be tested in London in the coming months and years. The GLA must seek to maintain the focus of this city-wide group on this critical risk to organisations in the city.

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

We set out the impact of the attack on the public, and the staff of both TfL and the GLA. We particularly thank the TfL and GLA teams who worked long hours in challenging circumstances to ensure that the cyber attack did not incapacitate TfL or the GLA, and to implement emergency measures to re-set staff accounts and ensure their colleagues could carry on with their own core roles. Recovery since that time has been mixed, with public-facing systems recovering quickly, while some GLA systems only returning to function a year after the incident. In this context, we welcome that TfL held an Independent Review, which should be critical in assuring the leadership of both TfL and the GLA that the lessons of this alarming cyber attack have been fully realised. Very little information about the findings of this review have been publicly released, we request that TfL share the report and a confidential briefing, with this committee.

Recommendations

Recommendation 1

By the time of the Annual Budget process for 2027-28, 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.

Recommendation 2

As part of confidential risk updates to their board, the GLA and each functional body should introduce in 2026 reporting on the use of, and perceived risk level attached to:

a) specified IT 'legacy systems'
b) organisations within its supply chain with access to internal systems.

Recommendation 3

In response to this report, the GLA should confirm whether it requires its supply chain organisations to have completed the NCSC's Cyber Essentials Plus.

Recommendation 4

The GLA should set out in response to this report how effectively its HR and training systems monitor the staff completion of the new cyber security training. The GLA and all its functional bodies should review the optimum regularity of staff training, given the speed at which cyber risks emerge and change.

Recommendation 5

The GLA and TfL should in response to this report provide an update on what work is underway to understand 'workarounds' currently in use at the GLA, and the reasons behind any GLA user non-compliance with formal IT and cyber security processes.

Recommendation 6

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. It should report back to this committee on its findings.

Recommendation 7

In response to this report, both the GLA and TfL should confirm to this committee that all steps in the 2025 Cyber Assessment Framework 4.0 assessment have been completed and it has been adopted.

Recommendation 8

In response to this report, 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.

Recommendation 9

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.

Recommendation 10

In response to this report, the GLA should provide this Committee with a summary of its cyber security service agreements with TfL, including how it has articulated a minimum guarantee of digital / IT service to the GLA at times of emergency response and in the recovery period.

Recommendation 11

TfL should provide this Committee with the report(s) of the independent review of the TfL cyber attack. Representatives of TfL and the GLA should also provide a briefing to this Committee on the resulting implications and expected actions for both TfL and the GLA to ensure that lessons are learned and the cyber security risk is being fully managed for both organisations.

Cyber attacks: A revolution in crime

Speaking to journalists in London last year, the Secretary General of Interpol said that "The classical bank robbery is about to die out", explaining:

> "When I was a young police officer it was still that we needed to be strong and run fast to catch the criminal in a 100-metre race and should not wear glasses. In today's world, we need IT experts in the police and we're competing with the best IT companies for the best talents."[1]

One of our expert guests called cyber attacks a "revolution in crime"[2], one which requires urgent and ongoing attention to defend against.

For financial institutions, this is a new iteration of an old risk: banks have had elaborate physical security for hundreds of years. In today's world, online raids on bank accounts are now much more likely than an in-person bank robbery. The vast majority of frauds are also cyber-enabled.[3] Likewise, large and medium-sized businesses that handle customers' money and credit data are today much more likely to be subjected to a cyber attack than a physical breach of their building or threat to staff.

"they will go after anything on which they can find something useful, whether that is money or data or just disruption. Sometimes they do it for the thrills of doing it. In general, every organisation has to be more cyber aware and more responsive due to the fact that this world is changing."[4]

Shashi Verma, Chief Technology Officer, Transport for London
TfL

For public sector organisations, this has been experienced as a more novel threat. Councils and libraries did not used to experience bank robbery-like events; their buildings were not held up for the personal data in their filing cabinets. Councils' day to day operations, and local government staff, were not generally seen to be at daily risk of being halted by criminals intent on extracting a ransom before allowing them to go about their work.

[1] LBC, End of the bank robber? Interpol chief says criminals attack online and form gangs through dark web 'Yellow Pages' (2024)
[2] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p18
[3] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November, p5. See also The Little Book of Big Scams – 5th Edition [accessed 10 November 2025]
[4] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November, p4

Yet modern-day public sector organisations today face the same threat as banks and businesses do. In the online world, the collected personal data of citizens is valuable, and whole organisations' operations can be brought to a halt in order to extract a ransom. Recent cyber attacks on public sector bodies in London have paralysed those institutions – suspending normal operations for months and costing millions to recover.

Recent public sector cyber attacks in London: Case study 1

NHS Synnovis

In June 2024, an agency which managed pathology testing labs was the victim of a data hack. Synnovis provided blood testing services for two NHS trusts, several London hospitals, and GPs in Southwark, Lambeth, Bexley, Greenwich, Lewisham and Bromley.[5]

Ransomware hackers Qilin infiltrated the computer systems of Synnovis. It extracted data, and also encrypted vital information, rendering IT systems useless. It later reportedly shared almost 400GB of sensitive patient information on the dark web, including patient names, dates of birth, NHS numbers and descriptions of blood tests, as well as business account spreadsheets detailing financial arrangements between hospitals and GP services and Synnovis.[6]

Because the attack meant the NHS could not use some of its systems essential to run blood tests in south-east London, it also resulted in more than 6,000 hospital and GP appointments and operations being disrupted. In response to the attack, NHS England London declared a regional incident.[7]

The evolving threat

The most common form of cyber-attack is phishing, which the National Cyber Security Centre describes as:

> "when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information."[8]

The UK Government states that this is followed, to a much lesser extent, by others impersonating organisations in emails or online and then by viruses or other malware.[9] The Government's 2025 Cyber Security Breaches survey found that while the prevalence of cyber crime overall remained static, the number of businesses who experienced a ransomware crime in the last 12 months doubled in a year, increasing "from less than 0.5% in 2024 to 1% in 2025,

[5] NHS England, Synnovis Ransomware Cyber-Attack, date accessed 10 November 2025
[6] BBC News, Stolen test data and NHS numbers published by hospital hackers, (2024)
[7] NHS England, Update on cyber incident: clinical impact in South East London – Thursday 11 July, (2024)
[8] NCSC, Phishing: Spot and report scam emails, texts, websites and calls, page accessed 10 November 2025
[9] GOV.UK, Cyber security breaches survey 2024, (2024)

which equates to an estimated 19,000 businesses in 2025."[10] During this investigation, we heard how developments in AI mean attacks are increasing in both sophistication and volume, suggesting the threat will continue to grow and develop. Professor Madeleine Carr, Professor of Global Politics and Cybersecurity, University College London, told us that the technology enabling cyber crime had had an extreme effect:

> "Cybercrime is such a lucrative and relatively safe crime with the likelihood of being apprehended or charged comparative to the money that can be made. It is a revolution in crime, really, and the people who work in that field are unbelievably creative, talented and innovative."[11]

The Chief Executive of the British Library, which was a victim of a 2023 cyber attack, put the case even more strongly, stating: "The threat of aggressive and disruptive cyber-attacks is higher than it has ever been, and the organisations behind these attacks are increasingly advanced in their techniques and ruthless in their willingness to destroy whole technical systems."[12]

Major public sector cyber attacks in London: Case study 2

The British Library

In October 2023, the British Library (BL) was subject to a significant ransomware cyber-attack that compromised the majority of its online systems. The attack, which was claimed by the Rhysida ransomware group, exfiltrated data, encrypted or destroyed substantial portions of its server estate, and forcibly locked out all users from the Library's network. The BL stated in a later report:

"The criminal gang responsible for the attack copied and exfiltrated (illegally removed) some 600GB of files, including personal data of Library users and staff. When it became clear that no ransom would be paid, this data was put up for auction and subsequently dumped on the dark web."[13]

The Library said that alongside the release of personal data, the attackers had destroyed vital servers, stating: *"while we have secure copies of all our digital collections – both born-digital and digitised content[…] – we have been hampered by the lack of viable infrastructure on which to restore it."*[14]

A 2024 update stated: "The attack caused substantial damage that is complex and challenging to repair, beginning with the installation of a completely new computing infrastructure for the entire Library."[15]

[10] GOV.UK, Cyber security breaches survey 2025, (2025)
[11] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p18
[12] British Library, Learning lessons from the cyber-attack, (2024)
[13] British Library, Learning lessons from the cyber-attack, (2024), p2
[14] British Library, Learning lessons from the cyber-attack, (2024), p2
[15] Cyber Incident Update: Information & FAQ's - The British Library, accessed 8 September 2024

The Government's latest Cyber Security Breaches Survey estimates that UK businesses have experienced approximately 8.58 million cyber crimes of all types in the last 12 months (to April 2025). It states that over four in ten businesses (43%) and just under a third of charities (30%) in the UK report having experienced some form of cyber security breach or attack in the last 12 months. This was much higher for medium and large businesses (around 70%).[16]

Data from the Information Commissioner's Office (ICO) indicates that 3,116 cyber security incidents were reported to the ICO in 2024.[17]

"In fact, in many ways we could say that we are less secure now than we were 50 years ago."[18]

Professor Madeliene Carr, Professor of Global Politics and Cybersecurity University College London

As London's strategic authority, it is critical that the GLA grasps the scale of the cyber threat in London, and takes active steps to mitigate it. We set out to examine the risk to public sector organisations like the GLA in London, and to understand how the GLA is managing this risk.

During our investigation, TfL came under attack in September 2024, giving us real-time experience of the threat and the work required to mitigate it, which we consider later in this report. While we are reporting later than originally planned, this has allowed us to observe the developments in cyber security at the GLA and reporting on the TfL cyber incident throughout 2025.

[16] GOV.UK, Cyber security breaches survey 2025, (2025)
[17] ICO, Data security incident trends, accessed October 2025
[18] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p1

The public sector as a target

Public sector organisations are now routinely targeted by cyber attacks, with nearly half of all cyber incidents recorded in the UK between 2020 and 2021 being targeted at the public sector.[19]

Public sector organisations are targets for cyber crime for four main reasons identified in this investigation:

- First, they hold and process an abundance of sensitive data, such as citizens' personal information and critical infrastructure detail.
- Second, as these organisations have become increasingly dependent on data, computer systems and services for their day to day operations, they can be crippled by their IT going down (and thus theoretically vulnerable to a ransom demand).
- Third, attacks on public sector organisations can be very high profile, and for some criminal organisations and/or foreign state actors, disruption is the main aim.
- Finally, public sector organisations often do not have the resources of a bank or large private business to invest in cyber security. Some cyber-intelligence experts have warned that recent successful attacks highlight under-investment by the government, particularly in critical infrastructure such as schools, hospitals, and local authorities.[20]

As a result, the public sector is a target of threats ranging from cybercriminals [including hackers and organised crime] to potentially sophisticated espionage and sabotage schemes by foreign actors and terrorist groups.[21]

Local government as a target

The ICO records cyber incidents that result in a reported data breach. Since 2019, it has recorded 17,261 cyber incidents. Of these, there were 123 reported against central government, and over four times that - 494 - against local government.[22]

More recently, ICO data indicates that nine cyber security incidents were reported by Central Government in the first two quarters of 2025, while almost three times as many cyber security incidents were reported by Local Government (26) in the same time period.[23]

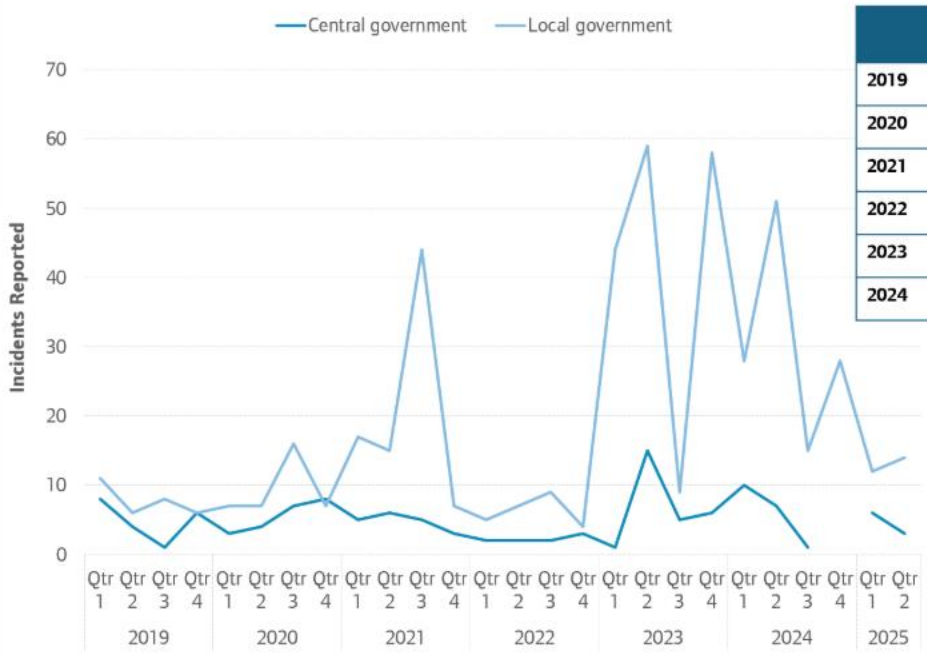
Professor Madeleine Carr told us:

---

[19] Cabinet Office, Government Cyber Security Strategy 2022-2030, 2022, p17 states: "approximately 40% of the 777 incidents managed by NCSC between September 2020 and August 2021 affecting the public sector."
[20] See, for example, Financial Times, Cyber attack on British Library raises concerns about lack of UK resilience, (2023)
[21] See, for example, Mi5, Countering State Threats, page accessed 10 November 2025
[22] ICO, Data security incident trends, accessed 1 December 2025
[23] ICO, Data security incident trends, accessed 1 December 2025

"It is common knowledge […] that local authorities and councils in the UK have suffered a number of very significant breaches and serious breaches. Part of what makes them attractive is that of course there is a lot of very valuable data held within these organisations, and data that fetches a good price in the criminal market. What makes them even more interesting and complex from a cybersecurity perspective are the very critical functions that are carried out by local government. Those are some of the implications that we have seen in Copeland [Borough Council] and in Hackney [Council], this shutting down of critical systems within society. There are very critical functions of local government and very valuable data that make them a target."[24]

Cyber incidents reported to the ICO by sector[25]



	Central Government	Local government
2019	19	31
2020	22	37
2021	19	83
2022	9	25
2023	27	170
2024	18	122

Major public sector cyber attacks in London: Case study 3

London Borough of Hackney (LBoH)

In October 2020, hackers attacked Hackney Council's systems – accessing and encrypting data, and withdrawing almost 10,000 records containing personal data in a massive ransomware attack. According to the Information Commissioner's subsequent investigations, the encrypted data included data on residents that revealed their racial or ethnic origin, religious beliefs,

[24] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p1
[25] ICO, Data security incident trends, accessed 28 November 2025. No data was reported for central government incidents in Q4 of 2024. The graph only reports on data security incidents that were discovered and then reported to the ICO.

sexual orientation, health data, economic data, criminal offence data, and other data including basic personal identifiers such as names and addresses. The hackers also deleted 10% of the council's backup before it was able to intervene. In January 2021 a criminal group posted some of the personal details of council staff and residents it had extracted on the dark web.[26]

The cyber-attack resulted in LBoH systems such as Council Tax, Business Rates, benefits, housing waiting lists, and Planning, all being disrupted for many months with some services not being back to normal until 2022.[27][28] Local press carried reports of the system processing the collection of council tax being "a mess", and there was considerable public criticism of the council.[29] The attack left a long legacy, with media reports in January 2025 alleging that Hackey had paid hundreds of thousands more than planned for IT consultants and staff to address the backlog in its systems.[30]

The ICO concluded its investigation into the breach in July 2024 and found that LBoH had failed to ensure that a security patch management system was actively applied to all devices, and failed to change an insecure password on a dormant account still connected to its servers, which was exploited by the attackers. An ICO spokeperson said:

"This was a clear and avoidable error from London Borough of Hackney, one that has resulted in a mass loss of data and has had a severely detrimental impact on many residents. At its absolute worst, this has meant that some of the most deeply personal information possible has ended up in the hands of the attackers. Systems that people rely on were offline for many months. This is entirely unacceptable and should not have happened.[…]

The council took swift and comprehensive action to mitigate the harm of the attack as soon as it learned it had taken place, including through their engagement with NCSC, and has taken a number of positive steps since.

There is a vital learning from this for both Hackney and for councils across the country – systems must be updated; you have to take preventative measures to reduce the risk and potential impact of human error and you must ensure that data that is entrusted to you is protected."[31]

The LBoH has disputed the ICO's findings and said that it did not breach its security obligations, and that the ICO had "mis-characterised and

[26] BBC News, Cyber attack costing six-figure sum, council says, (2024)
[27] ICO, London Borough of Hackney reprimanded following cyber-attack, (2024)
[28] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on, (2021)
[29] Hackney Citizen, Cyber attack: Hackney residents' anger over ongoing council tax 'mess', (2024)
[30] BBC News, Hackney Council still addressing 2020 cyber attack, (2025) and BBC News, Cyber attack costing six-figure sum, council says, (2024)
[31] ICO, London Borough of Hackney reprimanded following cyber-attack, (2024)

exaggerated" the risk to residents' data.[32] A year after the attack, the Mayor of Hackney Philip Glanville addressed the issues in a public statement, noting:

"The sad reality is that the damage to systems, the backlogs and the financial impact that residents are seeing is the ugly face of a growing global network of cyber criminals that choose to attack public servants delivering essential services. This wasn't just an attack on the Council – it was an attack on all of Hackney."[33]

In light of this rising trend of reported cyber incidents, in May 2024, the ICO called for all organisations to boost their cyber security and protect the personal information they hold, amid the growing threat of cyber attack.[34] In the next chapter, we consider how public sector organisations such as the GLA are doing so.

[32] Hackney Council, Response to Information Commissioner's Office cyberattack investigation, (2024)
[33] Hackney Council, Services available, but not back to normal – devastating impact of cyberattack one year on, (2024)
[34] IOC, Organisations must do more to combat the growing threat of cyber attacks, (2024)

Shoring up cyber defences in London

The National Cyber Security Centre defines cyber security as follows:

"Cyber security is how individuals and organisations reduce the risk and impact of cyber attacks.

Its core function is to defend the services we rely on and the devices we use – both at home and at work – from disruption, theft or damage. It's also about preventing unauthorised access to the vast amounts of data and personal information stored online and on these devices."[35]

In this report we do not set out the technical detail of the GLA's cyber security arrangements. This is for obvious security reasons, and also because it is not this Committee's place to assure the detailed operational and technical measures that make up an organisation's cyber defences.

However, given the seriousness of this threat for the GLA and its functional bodies, we set out to scrutinise the key actions taken by public sector bodies to prevent attacks, and the challenges to implementing them. In this chapter, we present some of the critical elements highlighted by our evidence for public sector cyber security.

Investing in defences

Cyber security is not cheap. The pace and volume of cyber attacks requires defences to be substantial, expert and ever-evolving to manage the developing threats. Given the level of investment required, it can be difficult for public sector organisations, including local government, to keep pace with equivalent private sector activity and spending.

The consequences of getting this wrong can be grievous; some commentators have blamed some of the recent successful cyber attacks on public sector organisations in London on under-investment by those organisations in their defences. The GLA's own written paper for this investigation referenced "constrained budgets for necessary upgrades" as one of the issues facing organisations.[36]

One area of expense is the cost of expert cyber-security salaries. Several guests spoke about this challenge, with Professor Madeleine Carr stating:

[35] NCSC Annual Review 2024, p. 7, accessed November 2025
[36] London Assembly Oversight Committee, Agenda for GLA Oversight Committee Meeting, Wednesday 27 November 2024, (2024), p72

> "There is a particular problem in organisations like this, which is that it is not possible to pay competitive salaries for IT staff and cybersecurity staff. That is not in any way to denigrate the people who do work in those roles here because I am full of admiration for them. They work under incredibly difficult conditions with a deep sense of responsibility for what their work means to the community."[37]

Shashi Verma, TfL, was likewise candid about the realities of this for TfL, stating that recruitment was "generally very difficult", and adding: "We are in a very competitive recruitment market. London has become a very significant technology hub with lots of technology companies, very often Silicon Valley companies that are paying a lot of money for technology [...] we have been able to build a very good team. Could it be even better? The answer is yes, it could be much better if we were able to pay people competitive salaries."[38]

"Technology recruitment has been a challenge for a long time. The cybersecurity space in particular is very hot. A shortage of skills nationally is well recognised and in many cases people with really high-quality skills will look to work for cybersecurity companies rather than for companies like us, for whom cybersecurity is a core activity, but we are not a cybersecurity company."[39]

Shashi Verma, Chief Technology Officer, Transport for London
TfL

One of the ways in which the public sector typically offsets a pay gap is by offering more permanent and stable positions than are sometimes available in the private sector. However, Professor Carr observed that this can actually be a problem for skills development in the case of cyber experts:

> "very often the way IT people, and cybersecurity people develop professionally is by moving to different organisations, encountering different systems and different problems and learning along those ways, and that does not tend to happen [in the public sector]."[40]

Dianne Tranmer, Executive Director of Corporate Resources and Business Improvement at the GLA, told us that the GLA's ongoing work on structuring its workforce ('Job Families') would help the GLA to understand and respond to both pay and career development in future by making IT and cyber roles comparable and accessible for people to move between the GLA and its functional bodies in their careers, stating: "because TfL will have more career development, and this is part of the rationale for IT shared services, you are bringing and pooling this series of experienced resources together."[41] At the time of writing, this work is still in development.

[37] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p6
[38] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p12-13
[39] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p12
[40] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p6
[41] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p13

More broadly, Shashi Verma, TfL, confirmed that financial institutions are able to invest more across the cyber security field, and argued that it was important to recognise that the public sector is delivering at scale, with far fewer resources than its private sector counterparts:

> "There is a need to recognise that, in this area, we are not competing with the rest of the public sector, we are competing with a private sector that is very well funded and recognises the financial risks and challenges around this much better. When you compare the cybersecurity expenditure that, for example, banks are undertaking, it is orders of magnitude different from what goes on in the public sector. When you look at the financial data alone that we hold, we run one of the world's largest payment systems, bigger than many banks. That recognition would be very helpful."[42]

While we acknowledge the truth of this point, we were then surprised by the difficulty we had in ascertaining from our guests how much other organisations, or even our own organisation, are spending in total on cyber security. Guests told us that this could not be easily quantified, as cyber security measures are often parts of wider IT or other systems.

It is clear that cyber security is critical to the GLA and its functional bodies, and requires funding that is commensurate with the risk, and that can compete with others in the sector. It is concerning that it was difficult to secure any clear numbers in terms of benchmarking the GLA's pay for relevant staff, or its overall investment in this critical function.

The kind of salaries and variety of experience that senior cyber security experts can achieve from banks and tech organisations will always be challenging to deliver in a public sector context. Alternative attractions that the public sector can offer, such as work-life balance, pension, and the opportunity to work on projects with national name recognition, have presumably already done much to secure the talent in the GLA and its functional bodies that is here today. However, the message to senior leadership is clear: paying more and investing in further cyber security staff, technology, and training would secure a better cyber security result. This has to be part of the cyber security conversation at the highest levels at the GLA and its functional bodies.

Recommendation 1

By the time of the Annual Budget process for 2027-28, 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.

Addressing legacy systems & supply chains

[42] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p14

Legacy systems

So-called 'legacy systems' have been identified as a problem in multiple public sector cyber security incidents. The term refers to the use of older software or hardware, which no longer has the latest technology and is potentially less supported by, or compatible with, current security systems. Such systems are therefore more vulnerable to a cyber attack. This is seen as a particular risk in public sector organisations which rely on older technology due to funding constraints.

For example, in its report on its own cyber attack, the British Library explained:

> "The Library's unusually diverse and complex technology estate, including many legacy systems, has roots in its origins as the merger of many different collections, organisational cultures and functions. We believe that the nature of this legacy infrastructure contributed to the severity of the impact of the attack. The historically complex shape of the network allowed the attackers wider access than would have been possible in a more modern network design, and the reliance of older applications on manual processes to pass data from one system to another increased the volume of staff and customer data held in multiple copies on the network."[43]

Some media sources commenting on the 2024 cyber attack on TfL said the organisation had been using old software vulnerable to attack, reporting that "one public-facing TfL system, still live on the internet today, is coded to be compatible with the Internet Explorer 6 browser, software which was last updated in 2008."[44]

When asked about TfL's use of legacy systems, Shashi Verma told us that TfL did 'retire' and remove legacy systems but the organisation's large scale was also a challenge for managing these:

> "The bigger challenge on the TfL side is our technology estate is vast. It is absolutely enormous. It is one of the biggest IT estates that any organisation runs in this country. The challenges of investment are endemic and that is true of all public sector organisations, very true of us as well. In our case, we run legacy systems going back to many decades. Keeping them safe is a challenge. There is always a challenge of keeping legacy systems safe. […], but it is a constant battle because these legacy systems are very well entrenched in the way our operations work and in many cases removing them is not cheap or quick. In the middle of all of our resourcing and funding challenges, finding the space to just remove legacy assets is very difficult."[45]

A later TfL Board paper in December 2024 further noted that legacy systems are a barrier to implementing the necessary 'zero trust architecture':

> "many public sector entities have yet to adopt robust zero-trust architectures, which is considered best practice in modern security, leading to unrestricted lateral movement within IT networks once attackers breach initial defences. Zero trust architectures assume that all external connections are hostile and verify each access attempt. Significant investment is required to migrate legacy technology systems to modern security practices."[46]

---

[43] British Library, Learning lessons from the cyber-attack, (2024), p3
[44] London Centric, Inside the Transport for London cyberattack, (2024)
[45] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p12
[46] TfL, Safety and Security Panel, 2 December 2024, (2024), p2

In evidence to us, Shashi Verma added that, as a result of the TfL incident in 2024 and the subsequent security system changes, many legacy systems will not work with the new systems and that "There is a bit of a forced cleanup going on right now."[47]

This can seem an obvious point on which to place blame: organisations are making themselves vulnerable by using older technology and they should update. However, our guests told us that this is not simple to address, either logistically or in terms of cost. Professor Carr used an NHS attack as an example:

> "For example, in the NHS - not the more recent Synnovis one but the WannaCry attack - there was a lot of blame on NHS IT staff. "Well, they should have done this", or, "How on Earth could they still be running Windows XP by this date?" However, the reality of these large public organisations is that the very expensive equipment that they had purchased could only run on Windows XP. To suggest that they replace those MRI scanners to update their Windows software just is not possible. It is not feasible."[48]

Professor Carr argued that this is a fault of the products on the market, rather than the organisations using them, stating:

> "we have believed particularly in the West now for 50 years that there would be some market drivers for cybersecurity, and that just simply has not emerged. There are two symbiotic markets: there is the market that quickly rushes software, hardware and services out and gets them in play, full of insecurities because no one really is buying these things based on security, and then there is the other side, the cybersecurity sector that comes along and mops up after them."[49]

Detective Superintendent Gareth Miles (Head of Crime, National Fraud Intelligence Bureau, City of London Police) recognised the same problem, but told us that there are still practical steps that organisations should take in this scenario:

> "Part of the problem that we see is that the networks that are contained within certainly public sector authorities are more of the elderly nature, as it were. Having the governance and the oversight to ensure that those networks are up-to-date and as secure as they can be, and then going on to the process of educating staff and limiting those attacks that get through, is an area that we could look at."[50]

In this context, both DSU Miles and other guests highlighted the importance of 'patching'- ensuring the latest security updates have been implemented in existing systems. This is a standard part of the cyber security defences, but is one that can be neglected, with catastrophic consequences. For example, DSU Miles said that the vulnerability used by attackers in the WannaCry attack against the NHS had already been identified by the time of the attack, and a patch to repair the vulnerability had been released six weeks before – but unfortunately had not been implemented on the NHS systems.[51]

---

[47] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p12
[48] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p5
[49] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p10
[50] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p2
[51] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p4

Considering the supply chain

A further concern identified by several guests was understanding and securing the 'supply chain' of an organisation like the GLA.

In this context, the supply chain refers to external partner organisations who are given access to some or part of the organisation's systems in order to do their work. According to Professor Carr:

> "As we have got better at hardening the perimeter of organisations and in that sense, we have improved cybersecurity to an extent, what attackers are doing is coming in through the supply chain. Many of these attacks now we see from these little, small organisations that we outsource different functions to."[52]

The GLA's written report states: "Recent large-scale cyber attacks have underscored these vulnerabilities and taught critical lessons. For instance, the 2023 ransomware attack on the British Library highlighted the importance of updating legacy systems and having robust incident response plans. Similarly, the 2024 Synnovis attack, which disrupted NHS services, demonstrated the risks posed by third-party suppliers, emphasising the need for comprehensive supply chain security."[53]

"Understanding the supply chain of an organisation like the GLA would be extremely difficult because it is not just the suppliers that are used by this organisation, it is the suppliers that the suppliers use and the suppliers that those suppliers use. It is a whole ecosystem of vulnerabilities."[54]

.

Professor Madeliene Carr, Professor of Global Politics and Cybersecurity University College London

The National Cyber Security Centre (NCSC) states that many organisations still struggle to manage supplier cyber risk and that "a lack of assurance tools, insufficient expertise and a lack of visibility are often cited as key barriers".[55] The NCSC offers its own cyber security certification scheme as one way for organisations to address supply chain risk, using a case study of a large financial organisation that asked its supply chain network of over 2,800 businesses to gain 'Cyber Essentials Plus' certification– the more rigorous version of the NCSC's cyber security certification scheme. It states that while complicated to implement, this resulted in 80% reduction in cyber security incidents for that business.[56]

[52] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p2-3
[53] Report of the Executive Director of Corporate Resources and Business Improvement to the Oversight Committee, 'Greater London Authority Cybersecurity', 27 November 2025 p. 78
[54] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p3
[55] NCSC, Cyber Essentials, page accessed 10 November 2025
[56] NCSC, Cyber Essentials, page accessed 10 November 2025

It is clear that both legacy systems and supply chains contain vulnerabilities that organisations such as the GLA must carefully manage. It is easy in the context of an attack to blame organisations for using legacy systems or outsourced partners, but there are clearly both practical and cost reasons for doing so, especially in constrained times in the public sector. Local authorities and public sector bodies must balance their spending on cyber security with their many other priorities, and it is not unexpected that they would continue to patch older systems if that is more cost effective. However, the risks are real and should be clearly understood by leaders making decisions about funding and approving operational plans.

Given how supply chains and legacy systems are a recognised vulnerability and are known to have been responsible for cyber incidents in London, it is vital they are the subject of regular reports to senior levels as part of organisational leadership's understanding of its own level of risk.

Recommendation 2

As part of confidential risk updates to their board, the GLA and each functional body should introduce this year reporting on the use of, and perceived risk level attached to:

a) specified IT 'legacy systems'
b) organisations within its supply chain with access to internal systems.

Recommendation 3

In response to this report, the GLA should confirm whether it requires its supply chain organisations to have completed the NCSC's Cyber Essentials Plus.

A culture of cyber security?

Both the GLA and TfL have thousands of staff using their digital and IT systems every day, few of whom are IT or cyber security experts. For most organisations, the most common cyber attacks still arrive through phishing emails and malware, to which anyone with an email address can be vulnerable. The extent to which staff are aware of the risks, and the broader way in which these staff interact with the hardware and software they use in their day to day jobs, is therefore of real importance to ensuring an organisation's cyber security.

"a culture where everyone is cyber-aware and takes ownership is one of the greatest defences against cybercrime."[57]

Dianne Tranmer, Executive Director, Corporate Resources and Business Improvement
Greater London Authority

We heard throughout our investigation how organisational culture and individuals' behaviour can be one of the greatest strengths in cyber security. On the other hand, a weak cyber security culture can create serious vulnerabilities for an organisation. All of our guests raised this as a key issue for the leadership of organisations to address. Dianne Tranmer, Executive Director of Resources at the GLA said: "The human factor cannot be ignored. Employees, contractors, and even trusted partners can inadvertently become entry points for cyber-attacks, often through phishing schemes or weak passwords."[58] Her written report to the committee emphasised this even more strongly, stating that "even the best technical defences can be undermined by human error".[59] Shashi Verma agreed that a culture of limited cyber awareness and inconsistent cybersecurity practices across teams leaves organisations vulnerable to phishing and social engineering attacks.[60]

The NCSC sets out the four 'essential activities' for organisations developing a positive cyber security culture: leadership; clear communication; simple reporting for incidents; and training. In this context, we considered how the GLA and its shared IT service provider, TfL, were doing to create a strong security culture.[61]

Staff training on cyber-security at the GLA

All our guests recognised staff training as important for cyber security. Dianne Tranmer told us that "Building a strong cybersecurity culture - where cyber resilience is viewed as everyone's responsibility and continuous training and vigilance are prioritised - is essential for ensuring that technical investments are fully effective."[62]

We have written separately to both TfL and the GLA about the details of their current staff training offer, which in the GLA's case has recently been updated.

In response to this report, the GLA should set out how it plans to assess the effectiveness of the new training, and also confirm that it will be able to provide comprehensive reports to this Committee on completion rates, and that individuals and/or their managers will be notified if they have failed to complete the mandatory cyber training.

---

[57] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p2
[58] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p2
[59] London Assembly Oversight Committee, Agenda for GLA Oversight Committee Meeting, Wednesday 27 November 2024, (2024), p72
[60] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p2
[61] NCSC Cyber Security Toolkit for Boards, p.14, accessed 10 November 2025
[62] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p2

Recommendation 4

The GLA should set out in response to this report how its HR and training systems will effectively monitor the staff completion of the new cyber security training. The GLA and all its functional bodies should review the optimum regularity of staff training, given the speed at which cyber risks emerge and change.

Leadership and communication on cyber-security

Both the GLA and TfL told us that they communicate regularly with staff on cyber risk, using what TfL termed "a multitude of different ways of pushing that message to the organisation", such as articles on the staff intranet and staff magazine.

Shashi Verma noted that there had been a 'silver lining' effect of TfL's latest cyber attack, in that it raised the profile of cyber security among all GLA and TfL staff.

"I would never wish a cyber incident on anyone but one of the things that this incident has done is raised the awareness of cybersecurity across the business. We forced a password reset on all accounts, but that also meant that my team that was doing the password resets went out to all operational sites and that was direct face-to-face engagement where people were able to talk about cybersecurity but also security in their own personal life. I would never wish a cyber incident on anyone but some good things did come out of it."[63]

Shashi Verma, Chief Technology Officer
Transport for London

Jules Gascoigne added that TfL tried "to identify different ways of engaging different groups around the organisation and to make the subject as accessible as possible for different groups and different individuals, everyone learns differently."[64] He added:

> "It is a challenge. It can be seen as something that is perhaps frightening or very complicated or very technical. What we try to do is make it clear that there are some fairly basic steps that everyone can undertake that will help protect themselves and the organisation and might also help protect them in their personal lives as well."[65]

'Cultural resistance' to cyber security measures

[63] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p9
[64] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p6
[65] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p6

We accept that both the training and engagement approaches are likely to be comparable to other bodies. However, we consider that the formal descriptions given did not always reflect our own experience of cyber security as members of this organisation. This disparity may be related to what the GLA's written report to us termed "overcoming cultural resistance" to cyber measures. [66] The GLA's written report and its verbal evidence both highlighted a perceived challenge of resistance among staff to efforts to improve cyber security.

"…while technical and cultural challenges play a role, overcoming cultural resistance and embedding cybersecurity into organisational values and daily operations are crucial to realising a truly resilient cybersecurity strategy."[67]

.

Report of the Executive Director of Corporate Resources and Business Improvement, GLA, to the GLA Oversight Committee

Shashi Verma took a pragmatic tone, telling us: "we are not relying upon perfection in terms of human behaviour".[68] When asked specifically about cultural resistance, he said "I do not think we face resistance in this. It is a question of where this lies in people's priorities against so many other things that they are required to do."[69]

This understanding of other priorities and demands of colleagues' main jobs is an essential insight, and one on which the GLA and TfL could reflect further. As the GLA looks to build a culture of cyber security, its leaders should not ignore the broader IT culture within the organisation, and the extent to which it enables people to feel supported and able to rely on the systems they use.

Anecdotal evidence suggests that the reality of some GLA staff experience is that the IT systems in this transition period [which remains ongoing] are not working seamlessly for them, and workarounds are perceived to be required in order to continue business as usual. We have written separately to TfL and the GLA about the impact of the transition process.

Improvements have been evident this year, for example in the reinstatement of remote working access and better access to an IT support portal. However, we still appear to be a significant way away from full systems integration and functionality. The organisation must make this accessible, for example, properly integrating systems to minimise vulnerabilities.

It is worth investing time in the relationship with staff using IT systems. The NCSC guidelines warn that a poor cyber security culture in which people do not engage with IT / Cyber colleagues leaves them less informed of key risks, stating:

> "Without a good security culture, people won't engage with cyber security, so [those responsible for cyber security] won't know about potential workarounds or unofficial

[66] London Assembly Oversight Committee, Agenda for GLA Oversight Committee Meeting, Wednesday 27 November 2024, (2024), p72
[67] London Assembly Oversight Committee, Agenda for GLA Oversight Committee Meeting, Wednesday 27 November 2024, (2024), p72
[68] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p8
[69] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p7

> approaches. Not only will you have an inaccurate picture of your organisation's cyber security, but you will also miss the opportunity for valuable employee input into how policies or processes could be improved."[70]

We did not hear self-examination among the GLA or TfL's shared service providers on why there would be "cultural resistance" in the GLA, or what the GLA/TfL was doing to understand why staff feel the need to implement 'workarounds' of systems. GLA and functional body staff must be responsible users of our technology and systems, ensuring passwords and devices are secure and up to date. However, the organisation is responsible for ensuring that its cyber security training and demands really align with the reality of how staff use the technology to do their jobs. Cyber security must not be simply something individual staff are told to do, but rather something that our systems facilitate them to do, and in trying to make our organisations more secure, it should not become more difficult for staff enact good practices.

This is an important reset moment for the organisation, and one which the GLA in particular must seize as an opportunity to launch a new cyber security culture after a period of disruption and transition. We urge it to do so.

Recommendation 5

The GLA and TfL should in response to this report provide an update on what work is underway to understand 'workarounds' currently in use at the GLA, and the reasons behind any GLA user non-compliance with formal IT and cyber security processes.

Maximising the potential for collaboration

A final point of focus from our evidence on how the GLA and other public sector bodies can increase their cyber defences was the prospect of better collaboration between organisations in the public and private sectors.

Experts who spoke to this investigation highlighted the possibility of cooperating more across the public sector in terms of sharing information about threats, challenges, and even sharing procurement. Ironically, security is one of the biggest barriers to sharing more of this information, as organisations are understandably wary to reveal risks and vulnerabilities, even to partners. Jules Gascoigne told us:

> "Over my time in the industry, the collaboration has improved, but there is still a long way to go. Earlier in my career, I found that organisations were extremely cagey about how they were operating and the incidents that they had been through. That is less the case now, but it is still the case to some extent, like Shashi is describing. That is because organisations do not want to reveal too much information. They might put themselves or their customers at risk or put them at risk of sharing information that they are unable to share because of the source of that information perhaps."[71]

[70] NCSC, Developing a positive cyber security culture, page accessed 10 November 2025
[71] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p5-6

Professor Madeliene Carr described how there was already some 'group learning' in the local public sector, though acknowledged that there were good reasons why there is not more co-operation. She nonetheless recommended that local government organisations could improve their cyber security "by increasing the market share, working together, sharing those lessons learned and having an ecosystem of your own that works for you in terms of procurement of those services."[72]

DSU Miles agreed, stating "Taking the learning is incredibly important and I do think it is happening. There are debriefs that go on in relation to large investigations and large cyber cases that are involved to identify the roots in the first instance."[73] He drew particular attention to the Cyber Resilience Centres in each region – London's being partially funded by the Mayor's Office for Policing and Crime.

Shashi Verma similarly told us that "there is a lot of cooperation […] We do talk to other organisations. We are part of many information exchanges, there are information exchange mechanisms set up between organisations. We are part of that. The NCSC is the coordinating body behind all of this and we work with them as well."[74] However, Jules Gascoigne indicated that TfL was still open to expanding its approach, agreeing that "there should be more collaboration. It is always better to share more information about controls that people are finding effective or the incidents that organisations are suffering."[75]

We note in this context that TfL board papers in 2025 have shown the organisation explicitly inviting shared learning from partners on cyber security, and even an openness to shared procurement on cyber security in future. TfL has also announced that it will share learning from the TfL cyber incident in 2024 with its partners. This is a welcome demonstration of continuous improvement in collaboration and we look forward to further information in due course.

[72] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p13-14
[73] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p6
[74] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p5
[75] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p5

GLA and TfL cyber security governance & resilience

Cyber attacks on organisations are now so common that leadership must consider an attack on their organisation to be inevitable. Representatives of both TfL and the GLA confirmed to us that cyber attacks are frequent, and that a bigger attack must always be expected, with Dianne Tranmer saying:

> "Cyber-attacks on the GLA take place daily, but they are recognised and stopped by automated firewalls and systems. It is increasingly a case of, not if, but when an incident will hit."[76]

Given this, cyber security must be a key focus for the senior leadership team in the GLA, and be a visible part of its governance structures. Our investigation considered how the governance structures at the GLA were understanding and responding to the cyber risk, and preparing a resilient response.

Prioritisation at leadership levels

Experts we spoke to during out investigation highlighted the importance of cyber security being understood at top levels of an organisation, and not just in its technical teams. DSU Gareth Miles told us that his key advice to organisations is to "strengthen their cyber governance and risk management and have appropriate frameworks and policies, and audit and compliance in relation to those policies."[77]

"…looking at Boards, do they understand that the resilience required in cyberspace is as important as the resilience required in their physical infrastructure as well? Sometimes the cyber aspect of it is -- not "ignored", "ignored" would be the wrong word, but it is not prioritised because of a lack of understanding, a lack of knowledge and a lack of realisation of what the impact is on an organisation if one of these offences take place."[78]

Detective Superintendent Gareth Miles, Head of Crime, National Fraud Intelligence Bureau, City of London Police

Both TfL and the GLA told us that cyber security received appropriate prioritisation in governance structures. Shashi Verma told us that that when he raised issues about cyber security at leadership levels "we are not being second guessed all the time. We are being asked difficult questions, we do not get away from scrutiny, but we are not being second guessed and I think that is really important."[79]

[76] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p1
[77] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p17
[78] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p5
[79] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p16

"In terms of governance, I do not think we have come across a point where we have asked for something to happen and it has not happened. The cybersecurity exercise that we ran with the executive was something that […] [had] the support of the entire organisation, [which] is a testament to the fact that the organisation takes cybersecurity seriously and it takes the competence of the people running it seriously."[80]

Shashi Verma, Chief Technology Officer
Transport for London

He also placed this in the wider context, recognising that there had to be a balance between "being able to let the organisation run while being safe."[81] He noted:

> "The challenge, to be fair, […] is it is not the only issue that the organisation is facing. This is one of a plethora of issues that we face every day, and therefore it is always vying for attention alongside many other things. Those other things are not unimportant. Physical safety is just as important, being able to run a day-today service is important, being able to be friendly to our customers is important. This is competing against many other things."[82]

Dianne Tranmer told us that the GLA took cyber risk similarly seriously, stating that "it has always been on as one of our top risks, it has been made more overt now just to highlight the controls and mitigations that we have in that area."[83]

Cyber security's place on risk registers

The TfL and GLA risk registers are one way in which the organisations can show that cyber security is a recognised threat and priority.

TfL said that cyber security was one of its top ten risks on its Corporate Risk Register which is "taken very seriously by our Board and by our executive. Not just because of this incident, it was taken very seriously even before."[84] Shashi Verma described a major cybersecurity exercise that he had run with TfL's executive about 18 months before the cyber incident.[85]

For the GLA, its risk register in early 2024 did not include cyber as a stated risk, but did include 'loss of data / wrongful access to GLA systems' as one of eleven sub-categories of a broader 'business continuity' risk. [86]

By October 2024 (one month after the TfL cyber attack), the GLA risk register was dramatically revised. The GLA's Corporate Management Team reported that "A new cyber security risk has

[80] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p16
[81] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15
[82] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15
[83] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15
[84] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15
[85] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15
[86] Risk register, GLA Papers to Audit Committee for its meeting on 2 February 2024

been included regarding the GLA's ability to safeguard assets and prevent severe disruption to service delivery through cyber attacks".[87] A new Cyber security risk was put at the top of the risk register, followed by a revised business continuity risk elevated to the second point on the list.[88] The recognition and articulation of the GLA's cyber risk has evolved further in more recent iterations of the register - these are discussed further in the section below.

We are satisfied that cyber security is now high on the agenda for corporate teams across the GLA and TfL - how could it be otherwise, given the profile of the TfL cyber incident in 2024. We welcome this awareness and focus, and would now like to see GLA senior management adopting a fluency and maturity in their approach to cyber security issues. For example. the GLA should confirm how often its CMT will discuss cyber security, and how it will use the revised risk register approach to drive improved security.

Additionally, the cybersecurity exercise that TfL had run prior to the incident appears to be both prescient and genuinely useful in its learning for that organisation. We suggest that a comparable one is held for the GLA.

Recommendation 6

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. It should report back to this committee on its findings.

The changes to the GLA's risk register were welcome, but it does appear to suggest that awareness was not as high in the GLA before August 2024 – in particular, awareness of how the other ongoing changes to IT systems through the shared services transition could result in impact on the GLA's cyber security. We consider that in more detail below.

IT Shared services- impact on cyber security

The GLA was somewhat insulated from the main effects of the September 2024 TFL cyber attack and resulting shutdown of systems. While GLA staff were required to re-set their devices, their email and access to documents and folders was not affected in days and weeks after the incident in the way that those of TfL staff were.

But this appeared to be largely because the planned transfer to the TfL IT estate was not yet completed. Dianne Tranmer provided a status update shortly after the attack, in November 2024:

> "We are partway through that transition. You will be aware that our infrastructure had been already outsourced to TfL. That remains the case. We still have - I do not know how to describe it - we have severed some of the connections and that means that we do need to reassess the IT shared services transition as we go through that. At this point in time, we have just halted the progress of the transition to the IT shared services while we all get our systems back together after the cyber incident."[89]

[87] Report of the Chief Finance Officer, 'Corporate Risk Register', to Audit Panel meeting on 17 October 2024
[88] Report of the Chief Finance Officer, 'Corporate Risk Register', to Audit Panel meeting on 17 October 2024, Appendix 1
[89] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p15

Shashi Verma recognised that it was a challenging point in the transition,

> "Any programme of this kind is challenging and moving IT from one organisation to another is challenging. […] Hindsight is a wonderful thing. Things could always have been done differently and so on. The important point here is that people are working together to do the right thing through what is not an easy transition. Being in this halfway house, where some of the transition has happened and some has not, is obviously not comfortable. Having an incident in the middle of that transition is obviously not helpful. We understand all of those points, but the core objective remains."[90]

The 'core objective' being the full integration of TfL and GLA IT systems into a single 'shared service'. A year later, this 'core objective' is still yet to be realised, which demonstrates the challenge and complexity of integration and the long term impact of the TfL cyber attack.

Both the GLA and TfL told us that the full integration of systems will improve the GLA's cyber security, by making it part of TfL's much bigger and better-resourced IT estate, and bring the GLA under TfL's cyber security protection. Shared service also raises the prospect of collective procurement, which our external expert guests had encouraged.

"…shared services definitely increase the complexity of systems. There is no doubt about that. I would ask you the opposite question, which is had the GLA been subject to a cyber-attack without the benefit of the dedicated cyber team and the dedicated technical teams that TfL has, what would the response have been? Shared services is adding complexity and I would not deny that at all, my team complain about it all the time, but it is also bringing benefits of a broader team, a more competent team, a more resilient team to both sides of the fence."[91]

Shashi Verma, Chief Technology Officer
Transport for London

While representatives of both TfL and GLA told us that they saw the shared service as a net gain for the GLA in the context of cyber security, we have noted that a recent report by the London Resilience Unit within the GLA highlighted the shared service as being a challenge for the Unit, causing difficulties for LRU staff in accessing IT accounts and exposing a broader risk for the future:

> "with all key resilience staff now operating on a single TfL system, rather than across two, the impact of any future system failure could be more widespread, potentially providing less operational resilience."[92]

We also note in this context that GLA risk registers were revised in 2025, in a manner that seems to indicate awareness of this issue. While in October 2024 the cyber risk was articulated

[90] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p16
[91] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p11
[92] London Resilience Unit: One-year evaluation and progress report, 25 September 2025

as: "The GLA fails to mitigate against a cyber attack and safeguard assets, causing severe disruption to delivery for Londoners";[93] by March 2025 it had been updated to read:

> "Our cyber security arrangements are highly dependent on our shared services arrangements where the GLA has little/no control, such that in the event of a cyber attack we fail to maintain or quickly recover our critical systems and data, severely disrupting the delivery of our services and programmes and fail to protect confidential organisational and personal data being obtained."[94]

And by October 2025 it had been refined further again:

> "Our cyber security arrangements are vulnerable to malicious activity due to high dependency on shared services over which the GLA has limited / no control, such that in the event of a targeted cyber attack or security breach, the structural reliance may prevent the GLA from effectively maintaining or rapidly restoring systems and data resulting in severe disruption to delivery of our services and programmes, and compromise the confidentiality, integrity and availability of sensitive organisational and personal data."[95]

As the move to fully implemented shared services has continued in 2025, it is critical that the potential cyber security implications and nuances are grasped by senior leaders at the GLA, and that it identifies any areas where the wider benefits are offset by specific new risks or challenges in key areas.

The cyber incident happening mid-transition to shared services highlighted both the downside and benefits of joining the bigger TfL estate. The reality of being tied in with TfL meant that GLA was affected in a way it wouldn't have been the year before. Moreover, the fact that the transition wasn't complete was unexpectedly positive: it meant the GLA was insulated from some of the worst negative effects in a way that it will not be once the transition is completed.

It is therefore understandable that the situation continues to cause some concern: the GLA has directly experienced the shared services downside in cyber security terms, and the consequences are ongoing as core systems used by GLA staff remained unavailable for up to a year after the incident. We welcome the GLA's revised risk assessments in this context.

Overall, we are persuaded of the upside: TfL clearly has more resources to defend an incident than the GLA had before. With the escalating cyber threat, this may prove important in future. However, TfL could now do more to reassure the GLA that its experience has been recognised, and the impacts on this organisation are taken seriously.

Cyber Assessment Framework

Both the GLA and TfL are operating within a broader national ecosystem of cyber risk and resilience management, in which the National Cyber Security Centre plays a key role. One of the main tools prepared by the NCSC to support organisations such as ours is the Cyber Assessment Framework (CAF).

---

[93] Report of the Chief Finance Officer, 'Corporate Risk Register', to Audit Panel meeting on 17 October 2024, Appendix 1
[94] London Assembly Audit Panel, Agenda for Audit Panel Meeting, Wednesday 17 March 2025, (2025), p73
[95] London.Gov, Appendix 1: Corporate Risk Register, (2025)

What is the CAF?

The Cyber Assessment Framework (CAF) is a tool to help organisations assess and improve their cyber security and resilience, managing cyber risks and protecting essential services from cyber threats.

Who is the CAF for?

The CAF is primarily designed for organisations operating essential services, in sectors such as energy, healthcare, transport, digital infrastructure and government. It supports both internal assessments and external oversight bodies, helping organisations meet legal and regulatory requirements like the NIS Regulations. It does this by providing a framework for assessing how well an organisation is meeting expected cyber security and resilience outcomes described within a CAF Profile.[96]

The latest version of the CAF [4.0] was released in August 2025.

For an organisation, the process of completing the CAF is a way to both ensure that it is complying with best practice as set out by the UK government, and also to demonstrate that it has fulfilled regulatory and legal requirements relating to cyber security. We asked representatives from TfL and the GLA if each organisation was CAF – compliant. TfL confirmed that it had completed the CAF,[97] while Dianne Tranmer told us that the GLA was in the process of doing so.[98] We note that in March 2025, the GLA's risk register actions noted that a new Knowledge and Information Assurance Working Group had been established "as a governance structure to ensure GLA remains proactive in managing information and cyber security risks, including evaluating the Cyber Assessment Framework (CAF)."[99]

Recommendation 7

In response to this report, both the GLA and TfL should confirm to this committee that all steps in the 2025 Cyber Assessment Framework 4.0 assessment have been completed and it has been adopted.

Resilience: planning for a cyber attack that restricts access to services

In addition to preparing to defend an organisation against cyber attack, we heard from experts how it is also important for organisations to also focus on becoming resilient to them when they do occur. Our guests asked organisations to consider how long they can carry out their critical functions without their IT systems, and to proactively plan for crisis events.

[96] NCSC, Cyber Assessment Framework, accessed October 2025
[97] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p.14
[98] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p10
[99] London Assembly Audit Panel, Agenda for Audit Panel Meeting, Wednesday 17 March 2025, (2025), p73

We anticipate that a cyber attack that limited the GLA's access to main systems of email, teams documents and shared drives would significantly limit the ability of the majority of staff to do core tasks. The GLA does not provide key services as councils do, so the impact on the public would be less immediate, but the impact of such a withdrawal of access on the business operations of the organisation would be profound.

DSU Gareth Miles told us that it was "really important that organisations proactively plan for cyber incidents, have the documentation in place and see that it is fit for purpose, undertake regular training exercises as a board, as staff, and cascading down, and also have continuous evaluation that is going on throughout the time."[100]

"There is more systemic thinking that is necessary and one of those things we have talked about a couple of times is this approach to resilience. An organisation can continue to carry out its critical functions without its systems for how long, and does everyone know how to do that? That is becoming more and more important. Ironically, as we become more interconnected and more automated, that is becoming more and more important."[101]

Madeleine Carr, Professor of Global Politics and Cybersecurity University College London

We asked the GLA and TfL about their resilience approach. Both have 'Gold' control structures in place for the immediate cyber response.[102] They also noted that the incident response plans they had in place from before the September 2024 cyber attach on TfL were both used and useful. TfL told us:

> "We had run a big cyber exercise with our executive in June last year [2023] and the learnings from that cyber exercise were incredibly useful when the incident started in terms of roles and responsibilities, in terms of the nature of response, in terms of who has the decision-making powers at what times. These are all things that organisations need to be very well exercised in."[103]

The GLA said that it did have a cyber incident plan beforehand, but that the TfL cyber attack did mean that it looked again at its cyber incident management plan and reviewed it with TfL. Dianne Tranmer added "I think we responded very well in terms of how we did it. I will not say we were always perfect; we were learning as we were doing it. We have reviewed that incident plan and we also have all our business continuity plans."[104]

We also hear about the specific challenge of resilience to cyber attacks, in that organisations need to assume a medium-long term process, rather than a single event it can recover from. Shashi Verma said:

---

[100] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p17
[101] London Assembly Oversight Committee, Meeting transcript: Panel 1, 4 September 2024, p19
[102] See Public Pack)Minutes - Appendix 1 - Item 8 - Transcript Minutes Supplement for GLA Oversight Committee, 27/11/2024 10:00 p19, and London Assembly Audit Panel, Agenda for Audit Panel Meeting, Wednesday 17 March 2025, (2025)
[103] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p11
[104] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p19

> "One of the things that makes an incident of this kind different from other safety incidents is that the incident never ends. On day one, day two, day three, even day ten, you do not know whether the incident is over or not. That uncertainty makes it very difficult to manage because the situation is changing almost continuously."[105]

While the CAF process supports organisations to ensure they have the best possible protection from a cyber attack, there is currently no common methodology for actually measuring an organisations' cyber *resilience*. As a result, UK Government departments and the NCSC have recently announced they are in the process of developing a new Cyber Resilience Index for measuring cyber resilience of key UK infrastructure across all critical sectors.[106] Given TfL's status as critical national infrastructure, and London's national importance, it seems reasonable that both TfL and the GLA should participate in this index process once it is available.

Overall, we found that information on the GLA's resilience planning for how it will handle a further serious incident (ie one that might affect the email system or files) is very limited. We assume this is because it would not be appropriate to publicly share this information, but we would welcome assurance to this Committee, and all GLA staff, that the senior leadership has in place tested and proven plans and contingency arrangements. This would also help demonstrate and bolster the organisational culture of cyber security that has been recognised as a key part of our defence.

Recommendation 8

In response to this report, the GLA should confirm that the GLA has tested and proven plans and contingency arrangements in the event of an incident that prevents staff access to emails and files.

The GLA's strategic role & London Resilience

The GLA's responsibilities relating to cyber risk and resilience go beyond its operation as an organisation. As a Category 1 responder under the Civil Contingencies Act, and leader of the London Resilience Group, the Mayor has significant responsibility for cybersecurity across all of London's public sector.

The GLA chairs the London Resilience Forum (LRF), which ensures London's preparedness in the event of emergencies and coordinates the activities of a wide range of organisations in the city. Following our investigation, and the TfL cyber attack, we were pleased to note that on 27 February 2025, the LRF held a 'strategic discussion' on Cyber Preparedness. According to minutes of the meeting:

> "The Chair introduced the strategic discussion on cyber-preparedness, noting that public sector organisations and their supply chains were increasingly under threat from cyber-attacks. Therefore, it was important for the partnership to consider how it protected itself from cyber-attacks and if an attack were to occur, how it would coordinate a rapid response to mitigate the impacts." [107]

[105] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p20
[106] Gov UK Cabinet Office, UK Government Resilience Action Plan, updated 14 July 2025
[107] London.Gov, Minutes – London resilience Forum, Thursday 27 February 2025, (2025), p4

The LRF also has a Cyber Working Group, which we understand will focus on raising awareness of the 2024 cyber response framework, networking across the partnership and breaking down silos between emergency planners and cyber security experts to improve preparedness for a major cyber incident.[108] We welcome this approach and necessary prioritisation at this high level forum of cyber risk and resilience, which is more than likely to be tested in London in the coming months and years. The GLA must seek to maintain the focus of this city-wide group on this critical risk to organisations in the city.

Recommendation 9

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 September 2024 TfL cyber attack

"On 31 August 2024, TfL was subject to a sophisticated cyber incident on our Information Technology Systems, resulting in the need to reduce access to the network and systems to minimise and contain the threat. Over the subsequent days and weeks, we took decisive action to contain the incident and recover control of the environment."[109]
TfL report

The TFL cyber attack in September 2024 took place just as this Committee launched its investigation into cyber security at the GLA. It was not the reason for, or focus of, this investigation, but it naturally featured in our consideration and our evidence. In this final section, we set out what information is publicly available about this attack, and how it impacted the GLA, which shares some of TfL's IT systems.

Summary of attack

TfL was subject of a network intrusion on 31 August 2024, and on 1 September reported "suspicious activity" on its systems. This went on to become a major cyber incident which TfL described as "sophisticated" and "aggressive".[110] It resulted in three months of disruption to TfL between September – December 2024, cost TfL an estimated £32 million to address, [111] and generated national and international headlines.

[108] London.Gov, Minutes – London resilience Forum, Thursday 27 February 2025, (2025), p4
[109] TfL, Safety and Security Panel, 2 December 2024, (2024), p2
[110] BBC News, Transport for London (TfL) cyber attack: What you need to know, (2024)
[111] TfL, Board Agenda, 26 March 2025, (2025)

Two individuals from London and the West Midlands were reportedly arrested and charged in September 2024 with conspiring to commit unauthorised acts under the Computer Misuse Act and fraud related charges.[112] Media stories indicate that they appeared in court in October 2025, and pleaded not guilty in November 2025, with a trial date set for June 2026.[113]

Detailed information about the attack and its perpetrators remains limited, particularly given the ongoing criminal case. The National Crime Agency (NCA) has previously stated that investigators believe the attack was carried out by members of the online criminal collective known as Scattered Spider,[114] the same organisation that we note has since been reportedly linked with attacks in the UK on retailers M&S and the Co-op.[115] Scattered Spider has been described by national cyber defence agencies as a cybercriminal group that targets large companies and their IT help desks, and which typically engages in data theft for extortion and uses ransomware.[116] However, there has understandably been very little information in the public domain about what exactly happened at TfL, and what organisations or individuals may have been involved. We do know that for TFL, the attack was considered one of the biggest challenges it has faced:

"Our Commissioner, Andy Lord, is on record as saying that he was in charge of major incidents at British Airways for 12 years. He is on record saying this is the worst incident that he has had to manage in his life. That gives you a sense of the enormity of what we were facing."[117]

Shashi Verma, Chief Technology Officer
Transport for London

Impact of the TfL attack

Public impact

For the public, the immediate effects of the September 2024 attack were quite limited. As part of its immediate response to the attack, TfL took direct action to shut down certain elements of its services to restrict the hackers' access to its systems. This affected live Tube information, online journey history, and payments on the Oyster app.[118] The tube and bus network continued to run as usual, though live Tube information was not available. The Dial-a-Ride assisted transit service for disabled people also had to temporarily suspend part of its operations.[119] However, as TfL told us, in comparison to other cyber attacks on large institutions, "in our attack, our core services kept on running, the Tube kept running, the buses kept running, all of our public transport kept running, and that is because of the very swift response that we enacted after the incident started."[120]

[112] NCA, Two charged for TfL cyber attack, (2025)
[113] BBC News, Teenagers appear in court over Transport for London cyber attack, (2025)
[114] NCA, Two charged for TfL cyber attack, (2025)
[115] Cybersecurity Dive, FBI, CISA warn about Scattered Spider's evolving tactics, (2025)
[116] CISA, Scattered Spider, page accessed 10 November 2025
[117] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p20
[118] TfL, Dial-a-Ride, accessed: 19 Sept 2024
[119] TfL, Dial-a-Ride, accessed: 19 Sept 2024
[120] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p11

A bigger and longer-term impact was felt by users of Oyster concession photocards including students, care leavers and apprentices, and Zip cards for children aged 11-15. TfL later said it had made the "difficult decision" to temporarily pause new concession photocard applications while it undertook "important security checks".[121] At the time, TfL invited people who wished to apply for these cards to continue making journeys as usual and keep a record of any fares paid, with the potential that they could claim it back later.[122] This was a significant challenge for many users of these cards, some of whom experienced real hardship as a result of having to pay full fares and then apply for, and await, a refund.

TfL re-opened applications for these concession cards throughout November 2024. When he spoke to us in November 2024, TFL's Chief Technology Officer could not provide a timeline for refund applications,[123] but in March 2025, we were pleased to note the Commissioner's report that TfL had "successfully cleared the remaining backlogs, processed more than 350,000 photocards, and issued interim travel refunds to customers who used alternative payment methods during the disruption."[124]

Two further notable impacts on the public included:

1) a delay to a new scheme to allow passengers to pay contactless for tickets at more stations across south-east England;[125]
2) A data breach for around 5,000 customers. TfL wrote later in September to inform affected individuals that there may have been unauthorised access to Oyster card refund data showing their personal information such as bank account numbers, emails and home addresses.[126]

Press coverage and criticism

Press coverage largely focused on the personal data breach[127] and also on the suspension of various travel cards[128] and the problems this had caused for Londoners. However, some reported more direct criticism of TfL, including allegations that its cyber security systems had not received adequate investment, and that it continued to use legacy systems running outdated software that made it vulnerable to such an attack.[129]

We asked TfL about this criticism, and officers acknowledged that there had been legacy systems in place [see Legacy section, above]. However, CTO Shashi Verma rejected any suggestion that TfL was in a vulnerable state:

> "I have to say that there is a fairly high degree of sophistication in the way that we have dealt with cybersecurity over the years. Despite the fact that this attack makes it look like we were vulnerable, every organisation is vulnerable. It is just a question of who gets on the radar of cyber criminals or potential hackers."[130]

---

[121] TfL Press Release 'Zip Photocard applications reopen for children and those aged 16+', 21 November 2025
[122] TfL, Cyber security incident, accessed: 19 Sept
[123] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p21
[124] TfL, Board Agenda, 26 March 2025, (2025), p15
[125] BBC News, Cyber attack delays pay-as-you-go train tickets in Kent and Surrey,(2024)
[126] TfL, Cyber security incident, accessed: 19 Sept
[127] The Standard, TfL cyber attack: Thousands of passengers feared to have bank details exposed as teenager arrested, (2024)
[128] BBC News, TfL photocards still unavailable after cyber attack, (2024)
[129] London Centric, "An utter shitshow": Inside the Transport for London cyberattack, (2024)
[130] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p5

He added that TfL had "had joint sessions with the NCSC, including our senior executive, after the incident where they have given us their view of our cybersecurity and how we dealt with it. They are on record publicly as saying that we dealt with the incident really well. That is not an easy accolade to come by it is very, very rare for the NCSC or the NCA to issue a public commendation of that kind, but they have done that in our case."[131] This point was echoed in the TfL's Commissioner's report in December 2024, which stated that "Partners (including the NCSC, NCA and Microsoft) have stated their view that we responded well to the incident and disrupted the attack to some extent, potentially preventing a far worse outcome."[132]

Impact for staff of TfL and the GLA

The cyber attack had a substantial impact on the staff of both TfL and the GLA. At the time of the attack, the GLA was in the process of migrating onto TfL's IT platform and systems as part of its 'shared services', so it was affected more than expected, but also less than it would have been if the migration had been complete.

For those staff in both institutions who were part of the team responding to the attack, it meant a long and stressful period enacting defences and determining appropriate responses on behalf of the organisations. For example, a major initiative was launched within 72 hours to re-set thousands of staff accounts, requiring a substantial in-person operation across several venues to conduct an "all-staff IT identity check" and reset hardware and accounts of every staff member. TfL commissioner Andy Lord thanked the thousands of TfL employees who have "really pulled together" in those weeks to address the disruption and maintain key services.[133] Dianne Tranmer told us in November:

> "I do want to acknowledge that the teams that work for GLA were around the clock and were absolutely exceptional. […] I cannot fault the work that they did and how hard they worked to support the GLA and all of our systems during that time."[134]

We echo these thanks to the TfL and GLA teams who worked long hours in challenging circumstances to ensure that the cyber attack did not incapacitate TfL or the GLA, and to implement emergency measures to re-set staff accounts and ensure their colleagues could carry on with their own core roles. As beneficiaries of the emergency process, we want to place our thanks on the record for a difficult job well done.

Following the immediate emergency measures, there were several key elements of IT provision that were withdrawn or changed as a result of the attack. These included:

- Limited or no access to the HR and finance systems for several weeks
- Delays / absences in hardware and software deployment, and work place adjustments.
- TfL shut off some key internal systems, including its "One London" online staff portal, which is used for email and web communications, and its internal system on which staff request holidays, reclaim expenses and arrange training sessions.

Many of these systems were recovered and reinstated within 1-2 months of the attack. However, the remote access system that previously allowed GLA staff to use internal finance and HR systems and shared network drives from home was disabled at the start of the attack, and a replacement was only implemented in September 2025, a full year after the attack. For

[131] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p5
[132] TfL, Commissioner's report: December 2024, (2024), p12
[133] TfL Board Meeting Agenda Report, 4 December 2024, p.8
[134] London Assembly Oversight Committee, Meeting transcript: Panel 1, 27 November 2024, p20

many GLA staff, the absence of a working remote access system meant regular inconvenience in accessing work systems, and/or a significant change in their working arrangements, as more tasks had to be done from the office.

While many other systems were recovered and restored quickly, it took over 12 months to restore the remote access service to key systems for GLA staff. We do not believe this delay has been adequately explained.

Recommendation 10

In response to this report, the GLA should provide this Committee with a summary of its cyber security service agreements with TfL, including how it has articulated a minimum guarantee of digital / IT service to the GLA at times of emergency response and in the recovery period.

Further investigation

The National Crime Agency and the NCSC investigations into the attack were ongoing at the time of this investigation, as was the criminal case. We hope and expect that more information and findings from these official investigations will be shared with the public at the appropriate time.

TfL also referred the data breach to the Information Commissioner's Office (ICO) for its investigation in September 2024. In February 2025, the ICO confirmed that it would not take any regulatory action against TfL as a result of the cyber incident and considered the matter closed, "unless new information comes to light that significantly changes its understanding of the incident."[135]

In the meantime, we note that TfL announced that it would conduct its own lesson learning exercise, stating: "Given the nature and scale of the cyber incident, an independent review will be conducted to consider the circumstances surrounding the incident and the impact, our response to the incident, and whether further improvements are needed to our cyber security strategy, taking into consideration existing initiatives that are in progress." [136] Notes from TfL's December 2024 Safety and Security Panel meeting state:

> "Not only is this appropriate from TfL's perspective, it is important to ensure lessons are learnt and shared particularly in the context of TfL's role in managing nationally critical infrastructure." [137]

We agree, and welcome this Independent Review, which will be critical in assuring the leadership of both TfL and the GLA that the lessons of this alarming cyber attack have been fully realised.

[135] TfL, Board Agenda, 26 March 2025, (2025), p41
[136] TfL, Board Agenda, 4 December 2024, (2024), p36-37
[137] https://board.tfl.gov.uk/documents/s23207/ssp-20241202-item-07-update on the tfl cyber-security-incident.pdf TfL, Safety and Security Panel, 2 December 2024, (2024), p4

The Independent Review was expected to be undertaken in phases, overseen by members of the TfL board. [138] The findings of the Review were expected to include recommendations to strengthen and improve TfL's cybersecurity and incident response.[139] TfL's board meeting reports throughout 2025 indicate that this vital review was undertaken by Bridewell, and has now been completed. The July 2025 TfL Commissioner's report stated:

> "The independent review highlighted areas of good practice. These included our skilled and dedicated staff across multiple areas, including Cyber Security, whose expertise played a significant role in minimising the impacts of the attack. It also highlighted that we acted quickly and decisively to protect our systems against further attack. […] We will address the learnings and recommendations identified from the independent review, which will be overseen by the Executive Security Group and reported to the Safety and Security Panel and Audit and Assurance Committee as appropriate. We will also share learnings with our incident response partners and wider stakeholders. The detailed report will remain confidential"[140]

No more detailed account of findings has been shared in public, although we understand that TfL has provided confidential briefings to specific Committee Chairs, including this Committee.[141]

Recommendation 11

TfL should provide this Committee with the report(s) of the independent review of the TfL cyber attack. Representatives of TfL and the GLA should also provide a briefing to this Committee on the resulting implications and expected actions for both TfL and the GLA to ensure that lessons are learned and the cyber security risk is being fully managed for both organisations.

[138] TfL, Board Agenda, 4 December 2024, (2024), p37
[139] TfL, Safety and Security Panel, 2 December 2024, (2024), p4
[140] TfL, Commissioner's report: July 2025, (2025), p6-7
[141] TfL, Board Agenda, 21 July 2025, (2025)

Committee Activity

Investigation aims and objectives

This investigation into Cyber Security at the GLA was launched in September 2024. It set out:

- 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.

Evidence gathering

Formal meetings:

The Committee heard from the following expert contributors during two formal meetings.

- **Meeting 1 (4 September 2024)**
    - **Professor Madeline Carr,** Professor of Global Politics and Cybersecurity, University College London
    - **DSU Gareth Miles,** Head of Crime, National Fraud Intelligence Bureau, City of London Police
- **Meeting 2 (27 November 2024)**
    - **Dianne Tranmer,** Executive Director for Corporate Resources and Business Improvement, GLA
    - **Shashi Verma,** Chief Technology Officer, TfL
    - **Jules Gascoigne,** Chief Information Security Officer, TfL

Informal meetings:

The Committee also held a private meeting on 27 November with the same guests as above.

Other formats and languages

If you, or someone you know needs this report in large print or braille, or a copy of the summary and main findings in another language, then please call us on: 020 7983 4100 or email assembly.translations@london.gov.uk

Chinese

如您需要这份文件的简介的翻译本，
请电话联系我们或按上面所提供的邮寄地址或
Email 与我们联系。

Hindi

यदि आपको इस दस्तावेज का सारांश अपनी भाषा में
चाहिए तो उपर दिये हुए नंबर पर फोन करें या उपर दिये
गये डाक पते या ई मेल पते पर हम से संपर्क करें।

Vietnamese

Nếu ông (bà) muốn nội dung văn bản này được dịch sang
tiếng Việt, xin vui lòng liên hệ với chúng tôi bằng điện
thoại, thư hoặc thư điện tử theo địa chỉ ở trên.

Bengali

আপনি যদি এই দলিলের একটা সারাংশ নিজের ভাষায় পেতে চান,
তাহলে দয়া করে ফো করবেন অথবা উল্লেখিত ডাক ঠিকানায় বা
ই-মেইল ঠিকানায় আমাদের সাথে যোগাযোগ করবেন।

Greek

Εάν επιθυμείτε περίληψη αυτού του κειμένου στην γλώσσα σας, παρακαλώ καλέστε τον αριθμό ή επικοινωνήστε μαζί μας στην ανωτέρω ταχυδρομική ή την ηλεκτρονική διεύθυνση.

Urdu

اگر آپ کو اس دستاویز کا خلاصہ اپنی زبان میں
درکار ہو تو، براہ کرم نمبر پر فون کریں
یا مذکورہ بالا ڈاک کے پتے یا ای میل
پتے پر ہم سے رابطہ کریں۔

Turkish

Bu belgenin kendi dilinize çevrilmiş bir özetini
okumak isterseniz, lütfen yukarıdaki telefon
numarasını arayın, veya posta ya da e-posta
adresi aracılığıyla bizimle temasa geçin.

Arabic

الحصول على ملخص لهذا المستند بلغتك،
فرجاء الاتصال برقم الهاتف أو الاتصال على
العنوان البريدي العادي أو عنوان البريد
الإلكتروني أعلاه.

Punjabi

ਜੇ ਤੁਸੀਂ ਇਸ ਦਸਤਾਵੇਜ਼ ਦਾ ਸੰਖੇਪ ਆਪਣੀ ਭਾਸ਼ਾ ਵਿਚ ਲੈਣਾ
ਚਾਹੋ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਇਸ ਨੰਬਰ 'ਤੇ ਫ਼ੋਨ ਕਰੋ ਜਾਂ
ਉਪਰ ਦਿੱਤੇ ਡਾਕ ਜਾਂ ਈਮੇਲ ਪਤੇ 'ਤੇ ਸਾਨੂੰ ਸੰਪਰਕ ਕਰੋ।

Gujarati

જો તમારે આ દસ્તાવેજનો સાર તમારી ભાષામાં
જોઈતો હોય તો ઉપર આપેલ નંબર પર ફોન કરો
અથવા ઉપર આપેલ ટપાલ અથવા ઈ-મેઈલ સરનામા
પર અમારો સંપર્ક કરો.

Connect with us

The London Assembly

City Hall
Kamal Chunchie Way
London E16 1ZE

Website: https://www.london.gov.uk/who-we-are/what-london-assembly-does
Phone: 020 7983 4000

Follow us on social media

LONDONASSEMBLY