Audit and Assurance Committee

Date: 29 November 2023

Item: Enterprise Risk Update – Significant Security Incident Including Cyber Security (ER04)

**This paper will be considered in public**

## 1 Summary

1.1 This paper provides an update of Enterprise Risk 4 (ER04) – Significant security incident including cyber security - which is accurately defined within the current threat environment and details the preventative and reactive controls and actions in place to manage our response.

1.2 A paper is included on Part 2 of the agenda which contains exempt supplemental information that is exempt from publication by virtue of paragraph 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to action which might be taken in relation to prevention, investigation, or prosecution of a crime. Any discussion of that exempt information must take place after the press and public have been excluded from this meeting.

## 2 Recommendation

**2.1 The Committee is asked to note the paper and the exempt supplementary information on Part 2 of the agenda.**

## 3 Current Status

3.1 TfL is an operator and owner of critical national infrastructure and plays a key role in the safety and security of London. We recognise the threat from deliberate, intentional acts to harm TfL and London’s people, reputation and economy is constant, evolving and increasingly significant in an unstable world. Financial crime, cyber-crime, organised crime, and the hostile actions of nation states are becoming indistinguishable. We adopt a holistic and risk-based approach to improve security and protect customers and our workforce from hostile and deliberate actions that cause harm.

3.2 We work to identify existing and emerging security risks and seek to reduce our vulnerability to terrorism, nation state hostile acts, extortion (through cyber-attacks), organised financial crime such as fraud, blackmail, corruption, espionage, sabotage, and industrial scale theft. Our systematic approach to protective security contributes to TfL’s and London’s sustainability.

3.3 Since the last update to Committee on 21 September 2022 we have continued to develop ER04 through a series of workshops with our internal and external security specialists.

3.4 ER04 has been developed to take a holistic approach to the security threats facing TfL. ER04 defines a significant security incident as the impact on TfL's operations, assets, customers, people, finances, and reputation caused from an incident or terrorism, sabotage, espionage, or serious financial crime. The scale and nature of the impact is a combination of a failure to sufficiently identify and understand the threats we face, or to recognise our vulnerabilities and seek to protect them, in order to deter, delay and detect such criminal activity. The causes fall within four broad categories: terrorism, sabotage, espionage, and serious financial crime.

3.5 This update expands the potential causes, adding activism (groups supporting political ideologies that may use activism to rally people around a particular cause, resulting possibly in cyber security incidents, demonstrations, graffiti, etc.) and the consequences and financial cost of a significant security incident happening, as well as the controls and actions in place to mitigate. The updated ER04 risk now reflects the preventative and corrective controls developed over the past 12 months.

3.6 These include ongoing delivery of a centralised Security Governance and Culture programme, which has brought about greater oversight of our risks at TfL and how we manage them. Regular reporting has been established on security matters to the Executive Security Group which represents all business areas within TfL to enable proportionate and effective decision making.

3.7 In June 2023, we launched our security strategy which builds on our corporate vision and values and sets out our path over the coming years up to 2030. Good security is the bedrock of a safe, reliable and successful transport system. We are working towards a future in which travelling in London and working for our organisation is and feels safe and secure and where our organisation is well protected against anti-social, criminal, malicious and hostile actions.

3.8 In September 2023, we conducted an incident response exercise which stress tested our response to a high-impact cyber-attack. Significant work was undertaken to better understand the potential impacts and mitigations under the given scenario. We identified a number of improvements to our processes as part of the exercise which will subsequently be incorporated into our incident response capabilities.

3.9 We recognise that everyone at TfL has a role to play in security and we actively work to increase awareness, understanding and competence through security training, briefings and acting on security communications.

3.10 ER04 provides oversight of the risk, causes, consequences and controls in place to manage it. Detail of this work is presented in the paper on Part 2 of the agenda.

**List of Appendices:**

A paper containing exempt supplemental information is included on Part 2 of the agenda.

**Background Papers:**

None

| | |
|---|---|
| Contact Officer: | Siwan Hayward OBE, Director of Security, Policing and Enforcement |
| Email: | siwan.hayward@tfl.gov.uk |