Audit and Assurance Committee

Date: **14 June 2016**

Item: **Cyber Security - Update**

This paper will be considered in public

1 Summary

1.1 This paper provides an update to the cyber security programme presented to the Committee on 8 March 2016.

2 Recommendation

2.1 **The Committee is asked to note the paper.**

3 Background

3.1 The purpose of the TfL Cyber Security team is to work in partnership with colleagues across the organisation to create resilience to cyber threats.

4 Coordination across TfL

4.1 Five principles for cyber security guide our constantly evolving approach. Those principles are:

(a) **Third Party Contracts** – Ensuring that the appropriate cyber security terms are contained in them.

(b) **Technical Controls** – Our technical controls align with the Centre for Protection of National Infrastructure (CPNI) 10. The CPNI 10, endorsed by the Cabinet Office, sets out ten practical steps towards resilience.

(c) **Threat** – We will be intelligence-led to manage and prioritise our vulnerabilities and threats.

(d) **Cyber Incident Response** – We constantly develop our processes for monitoring and remediating a cyber-incident in a timely way, learning from others.

(e) **People** – We ensure that our technology and data users are informed, trained and understand their specific roles and responsibilities.

Specific activities to support the principles

4.2 We have instituted a formal process to regularly review the roles and responsibilities of TfL staff that manage cyber risk, including third party contracts.

4.3 As part of our testing processes we hold cyber security exercises and further details are set out in Appendix 1. The next exercise is scheduled for 10 June 2016.

4.4 We are working to second a member of the British Transport Police to join the TfL cyber team.

4.5 We have strengthened our website protection.

4.6 We held a scenario based cyber security workshop that focused on future threats.

4.7 We have launched a cyber awareness campaign. The campaign includes posters, awareness reports, engagement and education with the operational teams, Yammer updates and question-and-answer sessions.

4.8 We developed a security schedule for contracts. The security schedule will be applied to three procurements for validation.

4.9 A “cyber readiness” statement will be required from suppliers at the Pre-Qualification Questionnaire stage of procurement.

4.10 A prime/subcontractor contact tree will be required of all contracts handling sensitive data.

5 Next Steps

5.1 We continue to develop the activities to support the five cyber security principles.

List of appendices to the report:

Appendix 1 – Overview of scenarios

List of Background Papers:

None

Contact Officer: Steve Townsend, Chief Information Officer
Number: 020 3054 0020
Email: SteveTownsend@tfl.gov.uk

Contact Officer: Michele Hanson, Chief Information Security Officer
Number: 020 3054 0020
Email: MicheleHanson@tfl.gov.uk

Overview of Cyber Security Exercises

The “Iron Bridge” cyber security exercise series follows a Gold, Silver, Bronze format. The exercises are presenter-led table top workshops that take the participants through a cyber-attack scenario. The scenario is based on a real-life incident and tailored to the threat profile of TfL.

The workshops provide a learning environment for decisions to be made and allow for discussion and debate at key junctures of the scenario.

The primary purpose is to exercise existing plans, policies, and procedures, or where they do not exist, highlight areas for further development.

The Iron Bridge exercises are developed with an increasing level of interaction with participants and complexity of threat.

Summary of last two exercises

Iron Bridge I, held in December 2015, focused on communication.

The key theme presented was the concept of chain of command, identifying who is responsible at different stages of a cyber security incident.

The scenario was based on breaking news relating to cyber-attacks against neighbouring fictional global cities.

The objective was to raise the perceived threat to TfL, and put the cyber security team on a heightened state of alert, and understand what that means e.g. what steps do we take.

The scenario stressed the importance of ensuring communications were managed both internally and externally. This includes our third party suppliers.

The scenario examined day to day security operations, and how security and TfL Online might interact.

Key discussions included when to escalate through the command chain and what should be communicated across the organisation.

Iron Bridge II, held in March 2016, built on the concepts from Iron Bridge I. Participants included London Underground, TfL Online, TfL Press, Information Governance, IM, Surface and British Transport Police. The scenario was tailored to ensure content of discussion was relevant to the new participants.

The scenario commences with a social media threat directed at TfL, followed by unauthorised modification of information displays/dot matrix boards on the underground.

The threat is related to a fictional activist group whose intent was to raise awareness of security failings in the transport sector.

The scenario culminated in the leak of data from CCTV and the corporate network, raising issues such as the classification and ownership of data.

The next exercise is on 10 June 2016.