Committees	Date:
Audit & Risk Management Committee Finance Committee	17 September 2015 22 September 2015
Subject: Cyber Security Risks	**Public**
Report of: Chamberlain	**For Information**

Summary

Cyber security and associated risks present a current and continuously evolving risk to the City of London Corporation and the City of London Police. The City Corporation has strengthened its audit activity in this area, drawing on appropriate internal and external expertise.

The Committee received a report in April setting out the cyber fraud risks facing the City Corporation and the City Police. The report summarised the potential vulnerabilities, possible audit activity and action being taken by management to minimise the threat of successful fraud. This report summaries the current position for the City Corporation and the City Police in respect of cyber threats. In particular it considers progress in respect of;

- Policy – a fully embedded Information Security policy, covering cyber security risks is in place at the City Police, whilst a comprehensive Information Security policy, likewise covering cyber security risks has been developed and is pending approval at the City Corporation. Employees have received adequate training to mitigate against the human risks to cyber security, through a programme of mandatory information security training.

- Department for Communities and Local Government (DCLG) guidance on cyber resilience - fully embedded at the City Police and comprehensively integrated at the City Corporation, with work in place to strengthen resilience in a small number of areas.

- Internal Assurance – internal assurance is to be gained by regularly re-assessing the extent to which cyber risks are reviewed as part of the Internal Audit work programme. Contracted IT service providers are required to meet specified security standards as defined by the City Corporation in business partnership contracts; this includes the requirement from Agilisys to ensure compliance with the PSN & PSNP requirements.

- External Assurance - the PSN (Public Secure Network) and PSNP (Public Secure Network - Police) external review process provides an appropriate level of assurance that the City Corporation and City Police networks are operating in a secure manner. Both the City Corporation and City Police are fully compliant with the secure network requirements and hold accreditation

from the Cabinet Office and Home Office respectively. Baker Tilley will be reviewing the City Corporation and City Police response to the DCLG guidance on cyber resilience in order to provide additional assurance.

Members are asked to:

- Note the report.

Background

1. Cyber security and associated risks are a growing issue for organisations, both within the public and private sectors; the City of London Corporation and the City of London Police are not exempt from these risks, and it is essential that the risks are understood, and robust controls are established to secure the City Corporation and City of London Police from these threats. The Committee received a report in April setting out the cyber fraud risks facing the City Corporation and the City Police. The report summarised the potential vulnerabilities, possible audit activity and action being taken by management to minimise the threat of successful fraud. Following on from the June Committee, the Internal Audit team was asked to establish what the current position is in relation to the measures in place to mitigate cyber threats.

Current Position

2. The Internal Audit team has conducted an initial review of cyber security requirements for both the City of London Corporation and the City of London Police and their position in relation to the key control framework requirements for cyber security, including Department for Communities and Local Government Guidance (DCLG), Public Secure Network (PSN & PSNP) requirements and Information Security policies, which incorporate cyber security. Findings have identified that the cyber security requirements for the City of London Police are far greater than those for the City of London Corporation, however it is essential that cyber risks for both organisations are managed effectively in order to mitigate the overall risks of attack.

<u>City of London Police Information Security Policy</u>

3. The City of London Police Information Security Policy outlines how the City Police safeguard and protect information assets from potential security threats with the following:
    - Information Security Procedures Manual
    - Acceptable Use Policy
    - Forensics Readiness Policy

4. The Information Security Procedures Manual covers information security threats, internal and external produced in line with regulatory requirements covering:
    - Information risk management regime
    - Secure configuration
    - Network security

- Managing user privileges
- User education and awareness
- Incident management
- Malware prevention
- Monitoring
- Removable media controls
- Home and mobile working

City of London Corporation Information Security Policy

5. The City Corporation's Information Security policy is currently in draft format and is pending approval by senior management. The policy covers information security threats, internal and external, produced in line with ISO 27002:2013 standards and guidance from the Information Commissioner, local Government, the Cabinet Office and other regulatory bodies. The policy includes:
    - User authentication
    - Device access and allocation
    - Remote access
    - Internet and social media
    - System access and use
    - Email access and use
    - Information sharing

6. The City Police's Information Security policy provides an established and developed response to cyber security risks, in line with the significant security requirements expected of a Police force. The City Corporation's draft Information Security policy represents a proportionate approach to cyber security risks affecting local government organisations.

7. The City Corporation and City of London Police have taken reasonable steps to ensure that employee's receive appropriate training to mitigate against the human risks to cyber security, through a programme of mandatory information security training.

Department for Communities and Local Government (DCLG) Guidance – Understanding Local Cyber Resilience, 10 steps to cyber security

8. We have benchmarked the cyber security response for the City Corporation and the City Police against DCLG guidance – Understanding Local Cyber Resilience, 10 steps to cyber security, issued in March 2015 (Appendix 1), which covers:

    - Information Risk Management Regime
    - Secure Configuration
    - Network Security
    - Managing User Privileges
    - User Education and Awareness
    - Incident Management

- Malware Prevention
- Monitoring
- Removable Media Controls
- Home & Mobile Working

9. The DCLG cyber security measures are fully embedded at the City Police, as would be expected for an organisation requiring significant security standards. The City Corporation, with a lower level of cyber risk, has measures in place in all key requirements, however a small number of additional measures have been identified where controls can be strengthened, these are;

   a) Finalise approval of the City Corporation's Information Security policy, which incorporates cyber security.
   b) Strengthen network access controls as an additional security feature.
   c) Ensure consistency in the application of processes for joiners, movers and leavers.
   d) Consider creating a central repository for system logs, gathering network data and enabling analysis and interrogation of suspect cyber activity.

External and Internal Assurance

10. The Public Services Network (PSN) is a UK Government programme to unify the provision of network infrastructure across the United Kingdom public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure.

11. PSN compliance requirements are designed to protect the organisations network. The Police Service Network in Policing (PSNP) scheme provides Police forces with improved security and accreditation to Home Office standards. Similarly, the compliance requirements for local Government, although not as extensive, also provide local Government organisations with improved security processes and procedures as set out by the PSN team, within the Cabinet Office.

12. The City Corporation (PSN) and City Police (PSNP) are compliant with the secure network requirements, and hold accreditation from the Cabinet Office and Home Office respectively. The PSN and PSNP external review process provides an appropriate level of assurance that the City Corporation and City of London Police networks are operating in a secure manner

13. PSN compliance is not the only way to deliver security across the organisations. Directing resources towards simply meeting PSN requirements is no substitute for engaging in ongoing risk assessment, management and mitigation across both organisations.

14. Both the City Corporation and City of London Police take reasonable steps, in addition to PSN requirements to monitor the networks for cyber threats.

15. A Police Service Risk Management Organisation annual report is produced and submitted by the City of London Police to the Home Office, in respect of cyber security risks. This includes an information assurance maturity model assessment performed against the following criteria with 1-5 rating
    - Leadership & Governance
    - Training Education & Awareness
    - Information Risk Management
    - Assured Information Sharing
    - Compliance

16. An inspection by the Information Commissioner considered the City of London Police to be exemplary in the cyber security work undertaken, and recommended that the City Police be an example for other forces to follow.

17. The City of London Corporation external penetration testing, conducted in January 2015, and detailed in the non-public report to this Committee in April 2015, provided additional assurance on the strength of the security controls adopted by the City Corporation in response to cyber threats.

18. The Internal Audit IT programme of work has been designed to review cyber associated risks, as set out in the cyber risks paper presented to this Committee on 28 April 2015. Internal Audit will continue to regularly review the programme of IT audit work to ensure that it accurately reflects the cyber risks affecting the City Corporation and the City Police.

19. Baker Tilley's IT Audit team will provide a further external check of conformity with the DCLG guidance for local cyber resilience and advise on the accuracy of policy and procedures covering cyber security.

20. Contracted IT service providers are required to meet specified security standards as defined by the City Corporation in business partnership contracts; this includes the requirement from Agilisys to ensure compliance with the PSN & PSNP requirements.

Conclusion

21 The City of London Police has developed and maintains a robust response to cyber related threats. The City Police response to cyber threats is in line with the expectations for an organisation holding sensitive and confidential personal data. The programme of annual external reviews for the City Police provides a strong level of assurance that cyber threats are being managed effectively.

22 The City of London Corporation has a proportionate response to cyber threats, it has achieved PSN compliance and is currently developing cyber related policy and procedure through the information security roadmap, which will provide the City Corporation with additional confidence that the threats posed can be managed adequately.

Appendices

- Appendix 1 – 10 Steps to Cyber Security
- Appendix 2 – DCLG Paper: Understanding Local Cyber Resilience (March 2015)

Chris Harris
Head of Internal Audit

T: 07800 513179
E: chris.harris@cityoflondon.gov.uk