Committee(s)	**Dated:**
Digital Services Sub Committee (DSSC)	January 24th 2020
Subject: CR 16 Information Security Risk	**Public**
Report of: Chamberlain	**For Information**
Report author: Gary Brailsford-Hart, Director of Information & Chief Information Security Officer	

Summary

The generally accepted definition of a data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual not authorized to do so.

CR16 was developed to capture and mitigate the risks a 'cyber breach' would present to the City of London Corporation (City Corporation). It is evident that dependent on the nature of the breach the impact can vary from very low to critical. Cyber threat is often viewed as a complex, dynamic and highly technical risk area. However, what is often at the root of a breach is a failure to get the basics right, systems not being patched, personnel not maintaining physical security, suppliers given too much information.

The National Cyber Security Centre (NCSC) 10 Steps to Cyber Security framework has been adopted to strengthen the controls in this risk area; this framework is now used by the majority of the FTSE350. The control scores are developing well and are reflective of the ongoing adoption across the City Corporation, all risk areas continue to be actively monitored and risk managed. Scores will continue to increase as improvements to people, process and technology are delivered.

The overall objective is to bring our security controls to an appropriate level of maturity. Currently, the organisation has a target maturity score of Level 4 (Managed and Measurable) across all areas, three controls are currently at this level, and seven control areas are currently at Level 3 (Defined Process). The mitigation controls are currently Amber (action required to maintain or reduce rating), with the ongoing improvements the CR16 risk is currently Amber. The risk score will remain Amber but should move to 8 from 12 by December 2020 based on delivering the target maturity scores.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Cyberspace has revolutionised how many of us live and work. The internet, with its more than 3 billion users, is powering economic growth, increasing collaboration and innovation, and creating jobs.

2. Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today. The City Corporation needs to be on the front foot in terms of our cyber preparedness. Cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it is.

3. Corporate decision making is improved through the high visibility of risk exposure, both for individual activities and major projects, across the whole of the City Corporation.

4. Providing financial benefit to the organisation through the reduction of losses and improved “value for money” potential.

5. The City Corporation is prepared for most eventualities, being assured of adequate contingency plans. This is tested annually with the work undertaken with the IT Health check and the National Government PSN accreditation. We have therefore adopted the NCSC Ten Steps to Cyber Security framework to assist and support our existing strategic-level risk discussions, specifically how to ensure we have the right safeguards and culture in place.

6. The creation of CR16 demonstrates the City Corporation’s commitment to the identification and management of this risk area.

Current Position

7. The development and implementation of an Information Security Management System (ISMS) was an essential requirement to permit the measurement and assurance of the CR16 risk. Several frameworks were considered, and the NCSC Ten Steps to Cyber Security framework, supported by the NCSC 20 Critical Security Controls, was chosen as the most appropriate for the City Corporation.

8. To provide an overview of CR16 risk management, the current compliance with the HMG Ten Steps assurance programme is detailed below (table 1) under each of the ten steps areas. The control scores continue to improve and are embedding across the City Corporation, the risk areas are actively monitored, and risk managed. Scores continue to increase as improvements to people, process and technology are delivered as part of the continuous improvement process. We have delivered and assessed the mitigation controls and believe that we have achieved an acceptable level of assurance. Furthermore, the risk management framework will reflect the controls as they mature within the organisation.

Table 1 - HMG Ten Steps assurance for the City Corporation as at Oct. 2019

Ten Steps - **Control Area**	% Complete	Target Score	Actual Score	Trend
1. Information Risk Management	86%	4	4	-
2. Network Security	69%	4	3	-
3. Malware Prevention	68%	4	3	-
4. Monitoring	72%	4	3	-
5. Incident Management	93%	4	4	-
6. Managing User Privileges	75%	4	3	-
7. Removable Media Controls	89%	4	4	-
8. Secure Configuration	86%	4	4	↑
9. Home and Mobile Working	71%	4	3	-
10. User Education and Awareness	75%	4	3	-

Options

9. Endorsement and support for the management and delivery of CR16 risk management plan has been obtained directly from chief officers as well as strategically via papers to Summit Group, Digital Services Sub and Finance Committees.

Proposals

10. Continue to implement the 10 steps programme across the City Corporation.

11. Continue to monitor threat, risks and harm and make recommendations for changing the risk status accordingly.

Implications

12. Failure to demonstrate appropriate controls in this risk area will expose the City Corporation to unacceptable levels of risk and could hinder several strategic objectives.

13. There are also several statutory requirements to consider for the management of this risk area, these are summarised at Appendix 3.

Health Implications

14. There are no health risks to consider as part of this report.

Conclusion

15. There is an extensive programme of work underway to mitigate the risks identified within CR16. This report articulates the work in progress and clearly

identifies where we will be directing continuing effort to manage this risk to an initial acceptable level and then monitoring as the controls mature across the organisation.

16. The breadth and scope of the necessary controls are cross-organisational and should not be entirely seen as a technical issue to be solved by the IT department. For example, if users leave the door open and their computers logged on then technical controls cannot in themselves defend the organisation.

17. The realisation of this risk would certainly have a severe impact on technical systems and directly impact the operational effectiveness of potentially the entire City Corporation. It is therefore imperative that the underlying issue of developing a security culture is supported through the delivery of risk controls for CR16. There is positive support for this work across the organisation and senior management understand and are supportive of the necessary changes to ensure the City Corporation's security.

18. It is important to note that whilst we are improving the CR16 risk position, it will only remain so with the continued operation and maintenance of the controls being put in place to manage it and should not therefore be considered a one-off exercise. The nature of the risk we face is illustrated with Appendix 6 the risk threat report. The risk score will remain Amber but should move to 8 from 12 by December 2020 based on delivering the target maturity scores.

Appendices

- Appendix 1 – CR16 Information Security
- Appendix 2 – Statutory Requirements Summary
- Appendix 3 – Maturity Scoring Matrix
- Appendix 4 – NON-PUBLIC - 10 Steps Detail Report
- Appendix 5 – NON-PUBLIC - 10 Steps Gap Analysis
- Appendix 6 – NON-PUBLIC – Risk Threat Report

Gary Brailsford-Hart
Director of information & Chief Information Security Officer
T: 020 7601 2352 E: gary.brailsford@cityoflondon.police.uk