Committee(s)	Dated:
Audit and Risk Management	23 May 2017
Subject: Deep Dive: 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 authorized to do so.

CR16 was developed as means to capture and mitigate the risks a 'cyber breach' would present to the 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 currently low and are reflective of the early phase of adoption across the City Corporation, the risk areas are actively monitored and risk managed. Scores will increase as improvements to people, process and technology are delivered throughout the year. The risk management plan is on target to deliver appropriate controls by the April 2018 review point.

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 actually 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. 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, Appendix 1, demonstrates the City Corporations 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 seen as an essential requirement to permit the measurement and assurance of the CR16 risk. A number of 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 a deep dive of CR16 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 are currently low and are reflective of the early phase of adoption across the City Corporation, the risk areas are actively monitored and risk managed. Scores will increase as improvements to people, process and technology are delivered throughout the year and we are currently on track to deliver mitigation controls by April 2018. Further detail is provided at appendix 2.

Table 1 - HMG Ten Steps assurance for the City Corporation as at May 2017

Ten Steps - **Control Area**	% Complete	Target Score	Actual Score
Information Risk Management	47%	4	2
Network Security	52%	4	3
Malware Prevention	57%	4	2
Monitoring	22%	4	1
Incident Management	73%	4	3
Managing User Privileges	39%	4	2
Removable Media Controls	46%	4	2
Secure Configuration	56%	4	2
Home and Mobile Working	25%	4	1
User Education and Awareness	36%	4	1

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, IT Sub and Finance Committees.

Proposals

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

Corporate & Strategic Implications

11. The City Corporation operates across multiple channels in multiple disciplines the common activity is the collection and processing of data into information. This information has a value, and we need to ensure we take appropriate and proportionate measures to ensure its security.

12. A number of local authorities have recently been targeted and have been compromised as a result. We are also aware of professional hackers launching a spear-phishing campaign directly against local authorities and their supply chains.

13. The City Corporation has not been immune to these activities and has suffered a number of cyber related security incidents over the past year. So far, the majority of these incidents have been minor in nature and easily managed locally.

Implications

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

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

Health Implications

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

Conclusion

17. There is an extensive programme of work required to mitigate the risks identified within CR16. This deep dive report articulates the work in progress and clearly identifies where we will be directing future effort to manage this risk to an acceptable level.

18. 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.

19. 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.

Appendices

- Appendix 1 – CR16 Information Security
- Appendix 2 – 10 Steps to Cyber Security Dashboard & Breakdown
- Appendix 3 – Statutory Requirements Summary

Gary Brailsford-Hart
Director of information & Chief Information Security Officer

T: 020 7601 2352
E: gary.brailsford@cityoflondon.police.uk