Committee(s)	**Dated:**
Audit & Risk Committee	16 July 2019
Subject: CR 16 Information Security Risk Deep Dive	**Public**
Report of: The 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 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 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 Measureable) 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.

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 demonstrates the City Corporations commitment to the identification and management of this risk area.

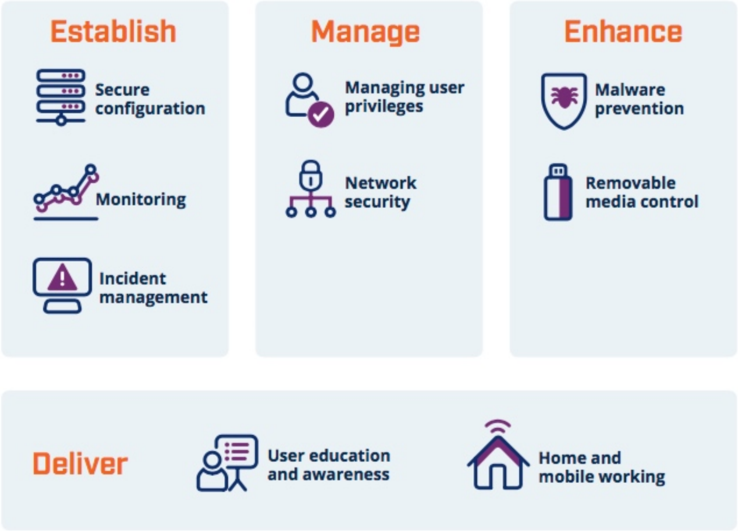
Current Position

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. The first step of the ISMS is the "risk management regime**",** as the NCSC describe it, this is the strategy that glues different controls and processes together. This ensures we do not fragment the approach to cyber security and identify hidden vulnerabilities and potential for compromise, ensuring the ability to measure the risk profile. The remaining nine steps are broken down into four clear delivery areas: Establish, Manage, Enhance, and Deliver.

Information Risk Management	% Complete	Target Score	Actual Score	Trend
Information Risk Management	86%	4	4	-

Risk appetite statement is the next applicable piece of work in this area. Involves an overarching agreement with the SIRO and then a cascade framework for application in each of the business areas across the City. In addition, a code of connection has been developed to support institutional departments connecting to and consuming core IT services from City.



Establish	% Complete	Target Score	Actual Score	Trend
Monitoring	72%	4	3	-
Incident Management	93%	4	4	↑
Secure Configuration	86%	4	3	-

The deployment, throughout October/November, of the Security Information and Event Management collector has taken place. However, connection work remains outstanding and once in place this will establish direct improvements to the monitoring and secure configuration across the City infrastructure.

Manage	% Complete	Target Score	Actual Score	Trend
Network Security	69%	4	3	-
Managing User Privileges	75%	4	3	-

Network security will directly improve following the implementation of the Security Information and Event Management collector was deployed throughout October/November. The issues of managing user privileges is currently being managed manually and a technical solution has been purchased and is awaiting implementation across the infrastructure – this is a complex piece of software and whilst installation is simple, the application and management will take time to develop and tune.

Enhance	% Complete	Target Score	Actual Score	Trend
Malware Prevention	68%	4	3	-
Removable Media Controls	89%	4	4	-

A project is underway to review the existing anti-malware solution and determine if enhancements are required, this has highlighted the need for anti-malware solutions for mobile devices. The removable media controls have recently been reviewed and the deployment of controls have been confirmed. To improve the removable media control score requires further work in respect of policies and user education, this is currently being included within the procedural refresh for removable media across IT, and this will include a sign-off process for receipt of device and responsibilities.

Deliver	% Complete	Target Score	Actual Score	Trend
Home and Mobile Working	71%	4	3	↑
User Education and Awareness	75%	4	3	-

The next steps for the Home and Mobile Working control area are for a thorough review of user acceptance policies and guidance. In addition, the aging Citrix infrastructure is being replaced, once complete this will improve the scores in this area. A developed schedule of awareness and training is being rolled out across the organisation with a different theme each month.

9. 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 June 2019 compared to March 2018.

Ten Steps - **Control Area**	% 2018	% 2019	Target Score	Actual Score	Trend
1. Information Risk Management	61%	86%	4	4	↑
2. Network Security	55%	69%	4	3	↑
3. Malware Prevention	57%	68%	4	3	↑
4. Monitoring	25%	72%	4	3	↑
5. Incident Management	75%	93%	4	4	↑
6. Managing User Privileges	54%	75%	4	3	↑
7. Removable Media Controls	46%	89%	4	4	↑
8. Secure Configuration	68%	86%	4	3	↑
9. Home and Mobile Working	36%	71%	4	3	↑
10. User Education and Awareness	46%	75%	4	3	↑

Conclusion

10. 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.

11. 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.

12. 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.

13. 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.

Appendices

Detailed Appendices available on request:

- Appendix 1 – CR16 Information Security
- Appendix 2 – Deep Dive - Dashboard & Breakdown

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