Committee(s)	Dated:
Digital Services Sub Committee (DSSC)	30th May 2019
Subject: CR 16 Information Security Risk	Public
Report of: Chamberlain	**For Decision**
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 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.

Recommendation(s)

Members are asked to:

- Note the report;
- Consider use of the Cyber Security Board Toolkit.
- Agree the recommendation to adopt the National Cyber Security Toolkit and a deep dive workshop to customise the toolkit for the City of London Corporation

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. Reducing the risk from a Corporate to a departmental risk does not reduce the amount of oversight from Officers and it would still be reported to the Members of DSSC for scrutiny and challenge.

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 (See Appendix 1). 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. This work is pending review of SIRO role and position within the business.				

Establish	% Complete	Target Score	Actual Score	Trend
Monitoring	72%	4	3	-
Incident Management	90%	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 remains ongoing. 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, this will include a sign-off process for receipt of devise and responsibilities.				

Deliver	% Complete	Target Score	Actual Score	Trend
Home and Mobile Working	64%	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 May 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	90%	4	4	-
6. Managing User Privileges	75%	4	3	-
7. Removable Media Controls	89%	4	4	-
8. Secure Configuration	86%	4	3	-
9. Home and Mobile Working	64%	4	3	-

10. User Education and Awareness	75%	4	3	-

Options

10. 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

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

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

13. Members are invited to consider changes to the reporting structure and method for CR16 in line with the Cyber Security Board Toolkit as provided at Appendix 2. and summarised below.

14. It is recommended that a deep dive workshop on IT Security using the toolkit is organised with Members of DSSC to develop new and broader metrics for developing further our security culture, protection and tools.

National Cyber Security Board Toolkit

Why have the NCSC produced a Board Toolkit?

15. Boards are pivotal in improving the cyber security of their organisations. The Board Toolkit been created to encourage essential discussions about cyber security to take place between the Board and their technical experts.

What can this toolkit do for the City of London Corporation?

16. Board members don't need to be technical experts, but they need to know enough about cyber security to be able to have a fluent conversation with their experts and understand the right questions to ask.

17. The Board Toolkit therefore provides:

- A general introduction to cyber security.
- Separate sections, each dealing with an important aspect of cyber security. for each aspect, it covers:
  - explain what it is, and why it's important
  - recommend what individual **Board members** should be doing

- recommend what the Board should be ensuring **our orgainsation** is doing
- provide questions and answers which we can use to start crucial discussions with your cyber security experts.

Getting started

18. The Cyber toolkit is more of a resource to be used to help us develop our own cyber security board strategy - one that can adapt to fit our own unique cultures and business priorities. It is suggested that Members start with the Introduction to Cyber Security for Board members and Embedding cyber security into our structure and objectives. (We are recommending a deep dive workshop)

How do cyber-attacks work?

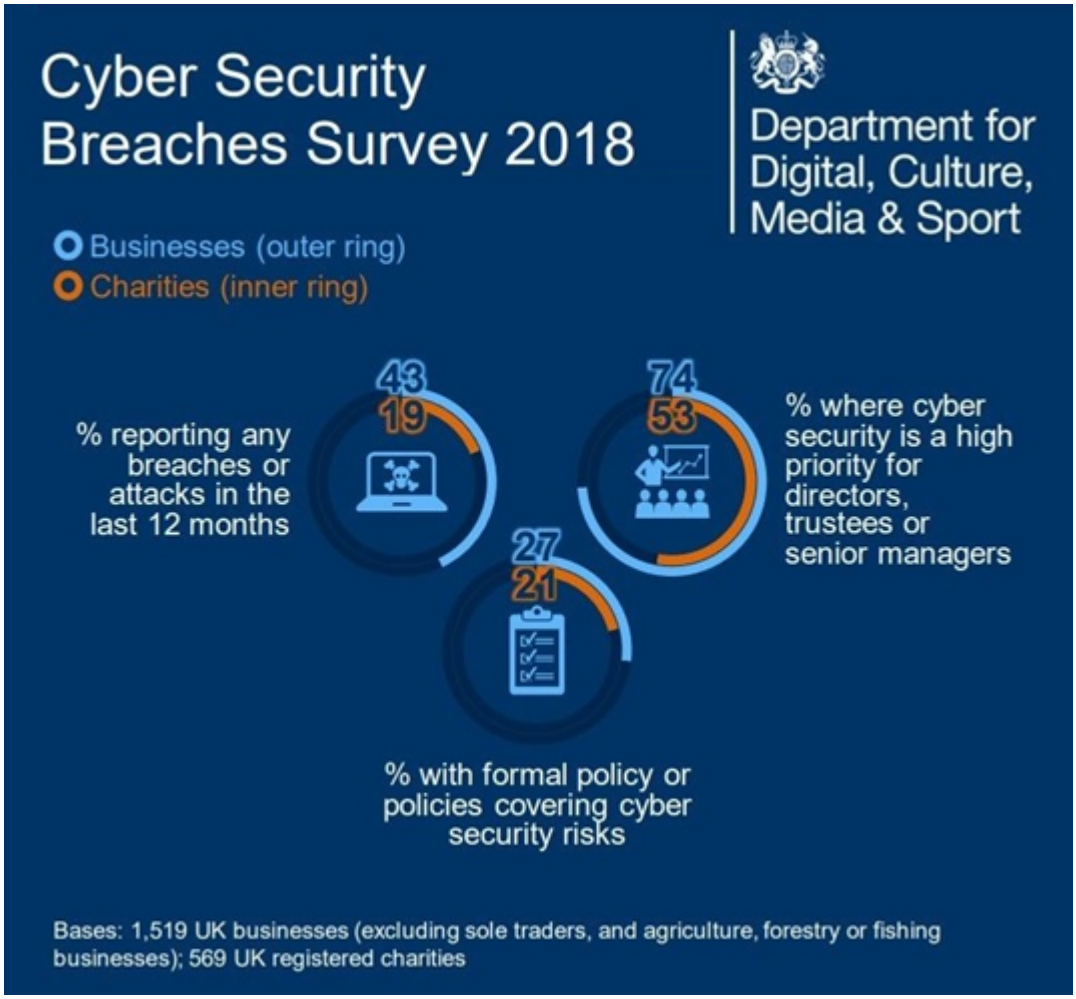
19. A good way to increase our understanding of cyber security is to review examples of how cyber-attacks work, and what actions organisations take to mitigate them.

    In general, cyber-attacks have 4 stages:

    - **Survey**- investigating and analysing available information about the target in order to identify potential vulnerabilities.
    - **Delivery** - getting to the point in a system where you have an initial foothold in the system.
    - **Breach** - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.
    - **Affect** - carrying out activities within a system that achieve the attacker's goal.

Defending against cyber attacks

20. The key thing to understand about cyber security defenses is that they need to be layered and include a range of measures, from technology solutions to user education to effective policies. The infographic below gives examples of defenses that will help our organisation to combat common cyber-attacks. The section on Implementing effective cyber security measures (see appendix 2) provides further detail and questions that Members can use to understand more about our own organisation's defenses.



Implications

21. 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.

22. The scale and types of Cyber attacks is illustrated in Appendix 3 – Cyber Threats Landscape report.

23. There are also a number of statutory requirements to consider for the management of this risk area.

Health Implications

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

Conclusion

25. 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.

26. 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.

27. 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.

28. 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 risk can be managed effectively as a departmental or corporate risk. It is for Members of DSSC to decide on the appropriate level of classification for the risk.

29. The recommendation is that we now adopt the National Cyber Security Board toolkit and customise our approach with this through having a deep dive Member's workshop.

Appendices

Detailed Appendices available on request:

- Appendix 1 – CR16 Information Security
- Appendix 2 – Cyber Security Board Toolkit
- Appendix 3 – Threat Landscape Report

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