Public Document Pack

CITY OF LONDON

Digital Services Sub (Finance) Committee

Date:	**THURSDAY, 30 MAY 2019**
Time:	**1.45 pm**
Venue:	**COMMITTEE ROOMS - WEST WING, GUILDHALL**

Members: Deputy Jamie Ingham Clark (Chairman)
Randall Anderson (Deputy Chairman)
Deputy Keith Bottomley
John Chapman
Tim Levene
Jeremy Mayhew
Sylvia Moys
Alderman Sir Andrew Parmley
James Tumbridge
Rehana Ameer
Deputy Hugh Morris

Full Committee Membership is to be confirmed at the Finance Committee on 21 May 2019.

Enquiries: **Rofikul Islam**
rofikul.islam@cityoflondon.gov.uk

Lunch will be served in the Guildhall Club at 1pm.
N.B. Part of this meeting could be the subject of audio or video recording.

John Barradell
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **MINUTES OF THE PREVIOUS MEETING**
To agree the public minutes and non-public summary of the meeting held on 5 April 2019.

For Decision
(Pages 1 - 8)

4. **OUTSTANDING ACTIONS**
Joint report of the Town Clerk and Chamberlain.

For Information
(Pages 9 - 10)

5. **FORWARD PLAN**
Report of the Chamberlain.

For Decision
(Pages 11 - 12)

6. **PRESENTATION FROM THE OPEN SPACES ON THEIR DIGITAL JOURNEY**
Director of the Open Spaces to be heard

For Information

7. **CHANGE AND ENGAGEMENT UPDATE**
Report of the Chamberlain.

For Information
(Pages 13 - 16)

8. **CITY OF LONDON CORPORATION INFORMATION MANAGEMENT EXECUTIVE SUMMARY**
Report of the Chamberlain.

For Information
(Pages 17 - 28)

9. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**
Report of the Chamberlain.

For Information
(Pages 29 - 34)

10. **IT DIVISION RISK UPDATE**
Report of the Chamberlain.

For Information
(Pages 35 - 40)

11. **IT DIVISION - IT DISASTER RECOVERY SUMMARY**
Report of the Chamberlain.

For Information
(Pages 41 - 44)

12. **CR 16 INFORMATION SECURITY RISK**
Report of the Chamberlain.

For Decision
(Pages 45 - 92)

13. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

14. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

15. **EXCLUSION OF THE PUBLIC**
MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Agenda

16. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
To agree the non-public minutes of the meeting held on 5 April 2019.

For Decision
(Pages 93 - 96)

17. **OUTSTANDING ACTIONS**
Joint report of the Town Clerk and Chamberlain.

For Information
(Pages 97 - 98)

18. **POLICING PROGRAMMES - UPDATE REPORT**
Joint report of the Chamberlain and the Commissioner of City of London Police.

For Information
(Pages 99 - 106)

19. **2020 SOURCING PROJECT UPDATES**
Report of the Chamberlain.

For Decision
(Pages 107 - 122)

a) 2020 IT Services Programme - Preparation of Tender (Pages 123 - 136)

Report of the Chamberlain.

20. **BLUE PAPER WEBSITE INCIDENT**
Report of the Chamberlain.

For Discussion

21. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

22. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

DIGITAL SERVICES SUB (FINANCE) COMMITTEE

Friday, 5 April 2019

Minutes of the meeting of the Digital Services Sub (Finance) Committee held at Guildhall, EC2 on Friday, 5 April 2019 at 1.45 pm

Present

Members:
Deputy Jamie Ingham Clark (Chairman)
Randall Anderson (Deputy Chairman)
John Chapman
Tim Levene
Jeremy Mayhew
Sylvia Moys
Rehana Ameer

Officers:

Rofikul Islam	-	Town Clerk's Department
John Cater	-	Town Clerk's Department
Sean Green	-	Chamberlain's Department
Matt Gosden	-	Chamberlain's Department
Sam Collin	-	Chamberlain's Department
Sammantha Kay	-	Chamberlain's Department
Ryan Dolan	-	Town Clerk's Department
Carol Boswarthack	-	Children & Community Services
Paul Hykin	-	Freemen's School
Gary Brailsford-Hart	-	City of London Police

In attendance:

Eugene O'Driscoll	- Agilisys
Ed	- Agilisys

-

1. **APOLOGIES**
   Apologies were received from Deputy Hugh Morris, Sir Andrew Parmley, James Tumbridge and Deputy Keith Bottomley.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were no declarations.

3. **MINUTES OF THE PREVIOUS MEETING**

   RESOLVED – That the public minutes and summary of the meeting held on 4 February 2019 be approved as a correct record.

4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
The Sub-Committee received a joint report of the Town Clerk and the Chamberlain outlining outstanding action from the previous meetings. The current outstanding action to be completed by the next meeting.

RESOLVED – that the Sub Committee:

- The report be noted.

5. **FORWARD PLAN - MARCH 2019**
The Sub-Committee received report of the Chamberlain concerning a forecast of events relevant to the Digital Services Sub Committee.

RESOLVED – that the Sub Committee:

- The forward plan be noted.

6. **CHANGE AND ENGAGEMENT UPDATE**
The Sub Committee received a report of the Chamberlain on the change and engagement update.

The Sub Committee was informed that there has been an improved service and the deployment of Microsoft Teams across the City of London Corporation, which is being utilised by over 600 members of staff. Members were further informed that work has started on upgrading the current Audio Visual (AV) equipment's and as part of the process, an installation of Skype Room system has been put in place in key locations such as the Chief Officer's rooms, Corporate meeting rooms and Committee rooms.

The Chairman asked about the use of IT in the overseas offices of the City of London Corporation. Senior members of Staff assured the Chairman and the Committee that currently, the Chamberlain is reviewing the IT services and its infrastructure of the overseas offices with an imminent meeting put in place with the City of London Corporation's Economic Development Office to discuss this further.

RESOLVED – that the Sub Committee:

- The report be noted.

7. **DIGITAL SERVICES SUB-COMMITTEE (DSSC) TERMS OF REFERENCE**
The Sub Committee considered the report of the Town Clerk on the Annual Review of the Sub-Committee's Terms of Reference.

A Member asked to add a section on the Terms of Reference covering the General Data Protection Regulation characteristic. The Chairman welcomed the comment and assured the Committee that the General Data Protection Regulation is covered within the Terms of Reference.

RESOLVED – that the Sub Committee:

- Subject to any comments and agreement approves the Terms of Reference of the Digital Services Sub Committee for submission to the Court (as a subset of the Finance Committee Terms of Reference) as set out in the appendix 1;
- Considers the frequency of meetings of the Sub-Committee; and
- Agrees that any changes to the Terms of Reference required in the lead up to the appointment of Committees be delegated to the Town Clerk, in consultation with the Chairman and Deputy Chairman.

8. **CR 16 INFORMATION SECURITY RISK**

The Sub Committee received a report of the Chamberlain on the CR 16 Information Security Risk. Members were informed that there has been an increase of Spear Phishing. Members have raised concerns on the same subject in the past with Officers from the City of London Corporation. Officers assured the Committee that this is being investigated.

Members were informed that the Information Commissioner, the watchdog responsible for data protection has fined Newham Council £145,000 due to its breach of information management and the way it was handled. Officers further emphasised the seriousness of such breach and the fact that large fines should focus the attention of councils, including the City of London Corporation and provides further incentive to ensuring that the City of London Corporation is up to date with all its Information Security Risks.

The City of London Corporation is addressing a wide range of potential Information Security Risks, as any failure to demonstrate appropriate control in such risk areas will expose the City of London Corporation to high-level risks and hinder various strategic objectives of the Corporation.

A Member asked why the dates we had on maturity levels were very broad and what were the intended maturity levels. Members were assured that the City of London Corporation has controls that allow the Corporation to monitor the progress on maturity levels. In addition, the City of London Corporation has a number of programmes put in place to mitigate any risks.

A Member asked if the City of London Corporation has plans put in place to respond to incidents without hampering any of the core services. The Committee were informed that the City of London Corporation designs its services with resilience in mind and makes every effort to avoid causing disruption to the services. As part of such services, there are testing and services in place to ensure that the City of London Corporation is prepared for the eventuality of disruption to service at present, the City of London Corporation runs its services through two different centres, working in partnership with Agilisys.

The Committee agreed that the Information Security Risk should remain as a Corporate Risk, as it is still live and remains as a constant risk. The Sub

Committee agreed to send a memorandum to the Chair of the Audit and Risk Management Committee on the importance of Information Security Risk remaining as a Corporate Risk. The Chairman noted the Chairman of Audit and Risk was receptive of such note.

A further report on Information Security Risk is to be tabled at the next meeting.

RESOLVED – that the Sub Committee:

- The report be noted.

8.1 **IT Division Risk Update**

The Sub Committee received a report of the Chamberlain on the CR 16 Information Security Risk.

RESOLVED – that the Sub Committee:

- The report be noted.

9. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**

The Sub Committee received a report of the Chamberlain on the IT Division - IT Service Delivery Summary.

There were discussions around the two incidents of interruptible power supply (UPS) due to the electrical apparatus that provides emergency power having failed to respond. This was due to the fact that the UPS are old and are not very well maintained. Responsibility for this equipment has recently been transferred to Digital Services and they will be updated and maintained on an appropriate schedule.

RESOLVED – that the Sub Committee:

- The report be noted.

10. **FREEMEN'S SCHOOL: IT MANAGED INFRASTRUCTURE SERVICE**

The Sub Committee considered a report of Roland Martin, Headmaster, Freemen’s School, as Chief Officer on the Freemen's School: IT Managed Infrastructure Service.

The school’s IT service is in use 24/7 by teachers, pupils, parent and guardians with a small team of officers based at the school providing the background support to the stakeholders. A Member suggested that the City of London Corporation’s IT team to work in collaboration with the school and provides support in terms of negotiating and managing contracts.

The City of London Police offered to work with the school and provide support around its IT security, which was welcomed by the school. Officers from the City of London Police IT services are in contact with the school and will be driving this forward.

Officers assured that the tender currently being prepared for the City's outsourced IT provision would permit the school to opt in to the services, if that was determined to be advantageous.

RESOLVED – that the Sub Committee:

- Approve combined G1-4 progression of project to G5;
- Approve recommended option (1); and
- Note total estimated cost of project of £530,000 over 5 years, all funded from Freemen's school fees.

11. **LIBRARY SELF SERVICE KIOSKS**

The Sub Committee received a report the Director of Community & Children's Services on the Library Self Service Kiosks.

There are three libraries across the City of London that provide services through self-service kiosks. These kiosks were acquired at different times and from different suppliers. Some are now out of support. The computers at the libraries provide free access to the internet and Microsoft Office. As the computers are currently connected to the public network, there is a vulnerability and reputational risk to the City of London Corporation of having unsupported kiosks.

Officers assured the Members that are restrictions put in place to prevent misuse and hacking occurring from the computers within the City of London Corporation's libraries and that the kiosks keyboards are not accessible by the public the machines are self-service, but they do not permit contactless payment, or in some instances any payment mechanism.

World Pay was suggested as a payment provider, as it is used by most other Local Authorities to receive payments for services. It was further explained to the Members that World Pay is a secure and easy to use kit.

The Chairman agreed that there are various payment processors and asked officers to find the right system for the City of London Corporation and report back to the Committee.

RESOLVED – that the Sub Committee:

- Approve Option 2 to source a new system, for proceeding to procurement and Gateway 4a;
- Approve the total estimated cost of £120,000; and
- Approve request for additional Capital budget of £70,000 to proceed to procurement and reach the next Gateway

12. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

There were no questions.

13. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

There were no items of urgent business.

14. **EXCLUSION OF THE PUBLIC**

MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

15. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
RESOLVED – That the Sub Committee:

- Approved the non-public minutes of the meeting held on 4 February 2019 be approved as a correct record.

16. **2020 SOURCING PROJECT - PROGRESS UPDATE MARCH 2019**
The Sub Committee received the report of the Chamberlain on the City of London Police IP Telephony and Call recording upgrade.

The Sub Committee received a presentation from the Director of IT on the City of London Corporation's vision 2020.

Members and Senior Officers also took the opportunity to thank the Chairman for his service to the Committee in terms of providing advice, leadership and steering the Committee forward.

Officers were praised for their hard work and service as the City of London Corporation was named as a recipient of the LGC's Highly Commended award for the Digital Impact award.

RESOLVED – that the Sub Committee:

- The report be noted.
- The Director of IT to share his presentation slides to Members.

17. **POLICING PROGRAMMES - UPDATE REPORT**
The Sub Committee received a report of the Chamberlain on the Policing Programmes - Update Report.

RESOLVED – that the Sub Committee:

- The report be noted.

18. **TRANSFORMATION UPDATE - COL & COLP**
The Sub Committee received a report of the Chamberlain on the Transformation Update for the City of London Corporation and the City of London Police.

RESOLVED – that the Sub Committee:

- The report be noted.

19. **WAIVER REPORT ORACLE LICENSING, SUPPORT & MAINTENANCE FOR FINANCIAL MANAGEMENT SYSTEM & PROPERTY MANAGEMENT SYSTEM FOR COL**

The Sub Committee received a report of the Chamberlain on the Waiver Report Oracle Licensing, Support and Maintenance for Financial Management System & Property Management System for the City of London.

RESOLVED – that the Sub Committee:

- The report be noted.

20. **CITY OF LONDON POLICE IP TELEPHONY AND CALL RECORDING UPGRADE**

The Sub Committee received the report of the Chamberlain on the City of London Police IP Telephony and Call recording upgrade.

RESOLVED – that the Sub Committee:

- The report be noted.

21. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

There were no non-public questions.

22. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

As part of the AOB, Members and Senior Officers took the opportunity to thank the Chairman for his service to the Committee in terms of providing advice, leadership and steering the Committee forward.

Officers were praised for their hard work and service as the City of London Corporation was named as a recipient of the LGC’s Highly Commended award for the Digital Impact award.

The meeting ended at 3.43PM.

Chairman

Contact Officer: Rofikul Islam
Rofikul.islam@cityoflondon.gov.uk

This page is intentionally left blank

Digital Services Sub Committee – Outstanding Actions- Public

Item	Date	Action	Officer(s) responsible	To be completed / progressed to next stage	Progress Update
1.	5 April 2019	CR 16 Information Security Risk	Director of IT	May 2019	The Committee agreed that the Information Security Risk should remain as a Corporate Risk, as it is still live and remains as a constant risk. The Committee agreed to send a memorandum to the Chair of the Audit and Risk Management Committee on the importance of Information Security Risk remaining as a Corporate Risk. Update: Being discussed at May Commmittee meeting.
	5 April 2019	Library Self Service Kiosks	Director of IT	May 2019	World Pay was suggested as a payment provider, as it is used by most other Local Authorities to receive payments for services. It was further explained to the Members that World Pay is a secure and easy to use kit. It was agreed that there are various payment processors and asked officers to find the right system for the City of London Corporation and report back to the Committee. Update: Research is still on-going into different systems that are being used in the City of London Corporation this will be reported at the July meeting.

This page is intentionally left blank

Forward Plan – May 2019

Report Title	Report Month	Category	Who
Presentation from DCCS	July 2019	Strategic	JA
IT Business Plan	July 2019	Strategic	SG
Digital Services Strategy CoL and CoLP	July 2019	Strategic	SG
Web Project Update	July 2019	Strategic	BR
Police Accommodation Programme Technology Roadmap Update	July 2019	Strategic	AB
Police National Programmes Update	July 2019	Strategic	AB
Presentation from Markets and Consumer Protection	September 2019	Strategic	AC
IT Operating Model Implementation Review	September 2019	Strategic	SG
Data Protection Policy Review	September 2019	Strategic	MC
Post 2020 Strategic IT Partner Procurement Update	September 2019	Strategic	KM
Smart Working Review	September 2019	Strategic	SC
IT Applications Roadmap	September 2019	Strategic	MG
Presentation from City Surveyors	November 2019	Strategic	PW
2020 Procurement Sign off	November 2019	Strategic	KM
Update on Information Management	November 2019	Strategic	SG
Web Project Update	November 2019	Strategic	MR
2020 Sourcing Contract Award Contract and Progress Reports at each meeting	TBA	Strategic	SG
IT Service Benchmarking Review	TBA	Strategic	SG
IaaS to Cloud Migration	TBA	Strategic	SG
Presentation from DBE	TBA	Strategic	TBA
Presentation from Economic Development	TBA	Strategic	TBA
Presentation from Town Clerks	TBA	Strategic	TBA
Presentation from Remembrancer	TBA	Strategic	TBA
Presentation from Comptroller	TBA	Strategic	TBA
Presentation from Barbican	TBA	Strategic	TBA
Presentation from CoLP	TBA	Strategic	TBA

Contributors
Sean Green – SG
Sam Collins - SC
Matt Gosden – MG
Andrew Bishop - AB
Kevin Mulcahy – KM
Sam Kay – SK

Gary Brailsford-Hart – GBH
Steven Bage – SB
Bob Roberts – BR
Jon Averns – JA
Paul Wilkinson – PW
Andrew Carter - AC

Agenda Item 7

Committee(s)	**Dated:**
Digital Services Sub Committee – For Information	30th May 2019
Subject: Change and Engagement Update	**Public**
Report of: The Chamberlain	**For Information**
Report author: Sam Collins, Head of Change and Engagement	

Summary

IT Transformation has already delivered £250,000 in cashable storage savings. To deliver further benefits requires the adoption of the Office 365 toolset that the organisation has already invested in with our Microsoft licence agreement. Tools such as Skype for business save time in travel with staff no longer having to travel to the City from our remote locations for short meetings and tools such as Sharepoint and Teams creating opportunities for more collaborative working.

Microsoft Teams is the latest office 365 tool now in use by over 1000 staff and presents a significant opportunity to improve ways of working for Departments as it combines collaboration tools such as Sharepoint, messaging and Skype into one single software solution. Adoption levels for SharePoint continue to increase month on month, though Skype for Business adoption has now stabilised and even reduced as some staff have moved from Skype to Teams. Work continues to upgrade the Audio Visual (AV) equipment and Skype systems in Chief Officer's rooms, Corporate meeting rooms and Committee rooms.

Recommendation(s)

Members are asked to:

- *Note the report.*

Main Report

Background

1. The desktop element of the IT Transformation Programme completed in February 2018, with the delivery of Windows 10 devices and Microsoft Office 365 to the organisation. Since that time, a programme of communications, training and campaigns has been delivered to drive user adoption and maximise the benefits from the organisation's investment in IT. The effective use of technology is increasingly important, as departments look to identify more efficient ways of working through the Fundamental Review.

User Adoption

2. The User Adoption Dashboard (delivered through PowerBI) continues to provide significant insight into City Corporation staff using the various technology elements;

   a. Around 1200 City Corporation staff are regularly using Skype for Business, though this figure has not increased in recent months

   b. Since its launch in February 2019, there are now around 1000 City Corporation Staff using Microsoft Teams (see fig.1).

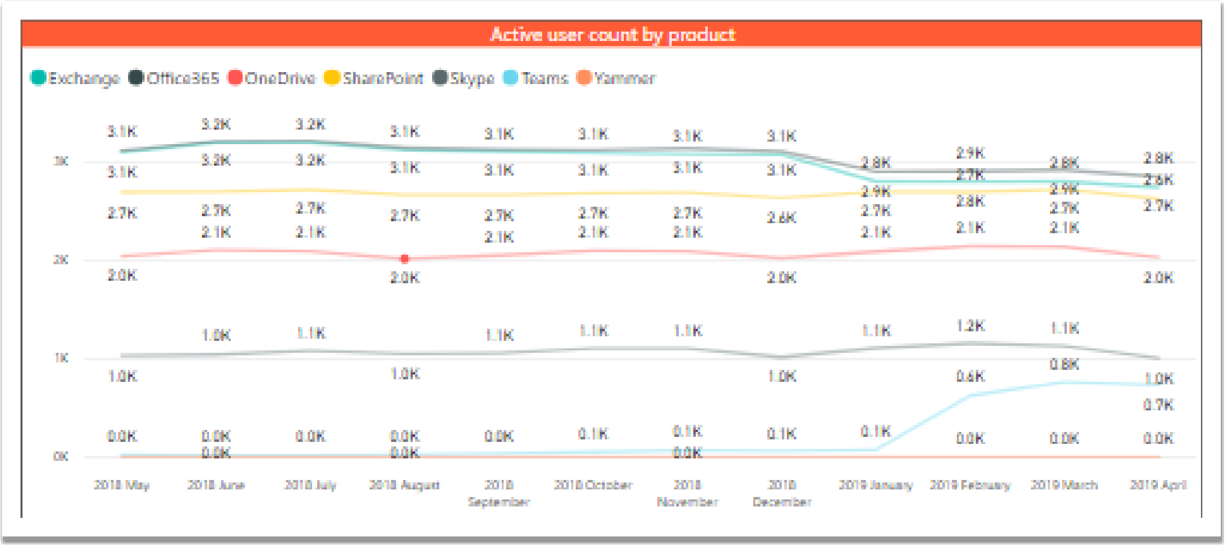


Figure 1

   c. The graph below (fig. 2), suggests that there has been a migration of communication activity from Skype for Business, to Microsoft Teams.

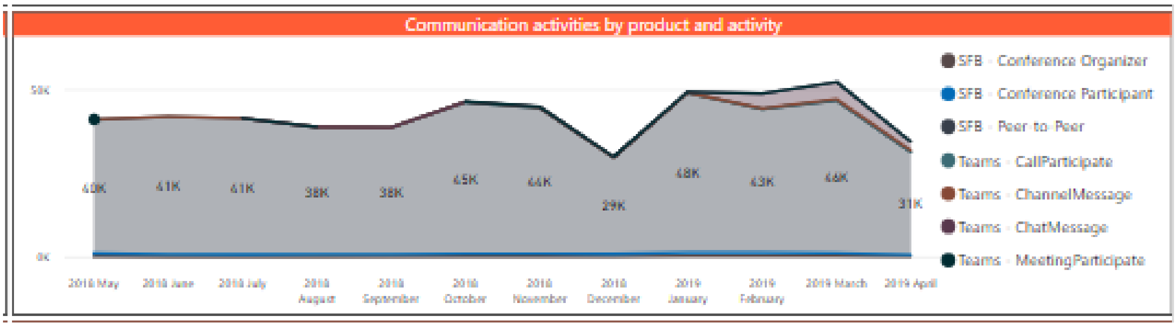


Figure 2

d. The number of active SharePoint sites across the organisation continues to increase – in April there were 333 active SharePoint sites, more than double the figure this time last year (fig. 3).

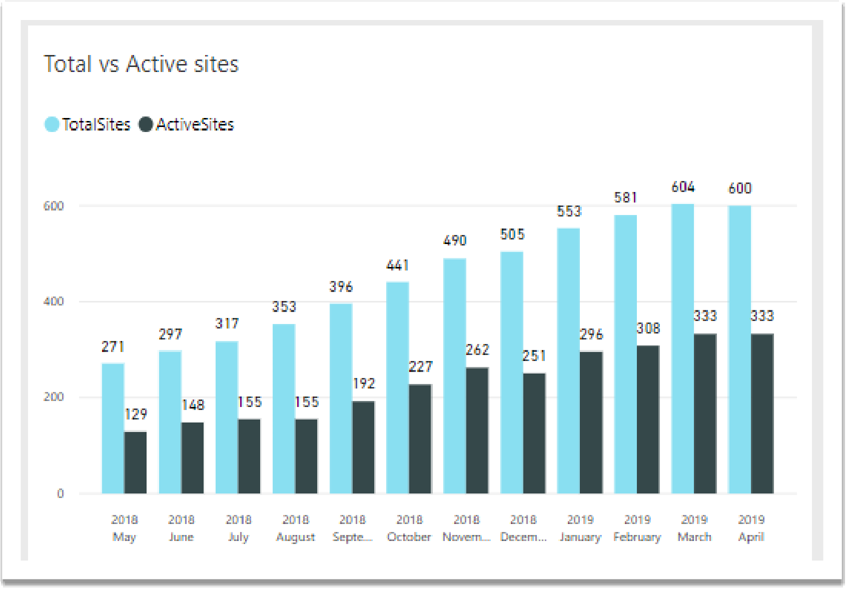


Figure 3

e. Chamberlain’s and Town Clerk’s continue to show the highest O365 adoption levels within the Corporation. Open Spaces and Markets and Consumer Protection show the lowest levels of Skype for Business and SharePoint adoption at present (see fig. 4).

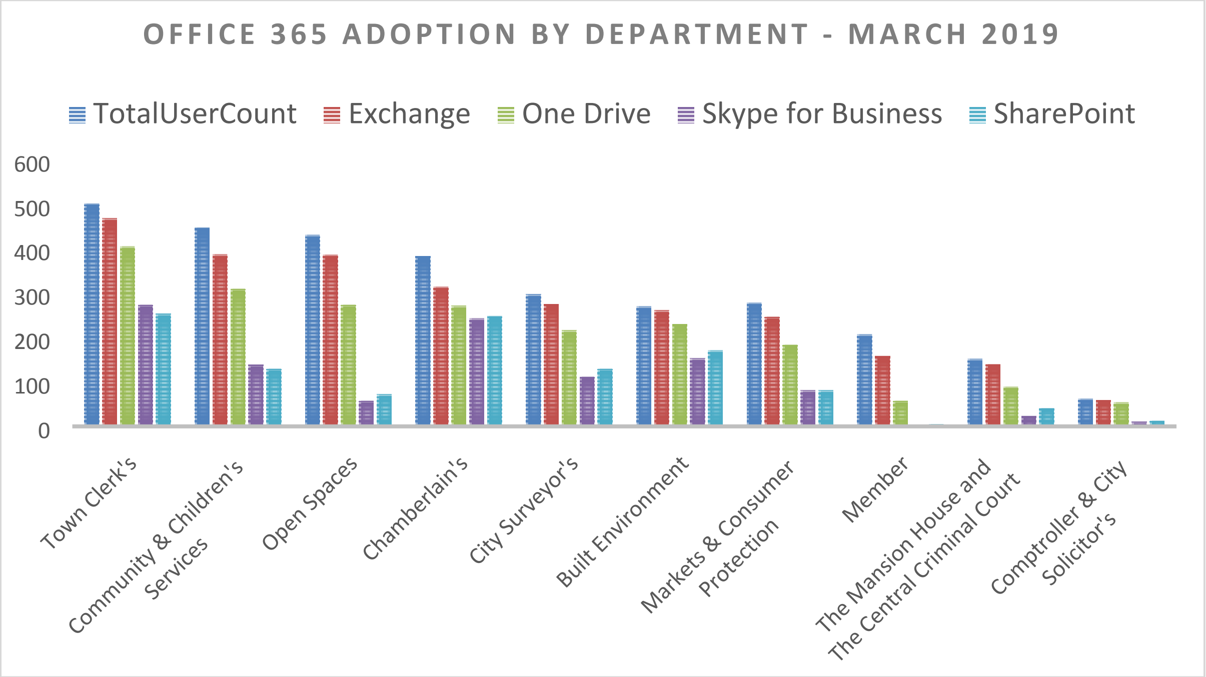


Figure 4

Skype Video-Conferencing Rooms

3. Skype Room Systems and display screens have now been installed across 8 office and meeting spaces in Guildhall. 3 further installations are planned to take place on 14th May.

4. Subject to appropriate funding, these will be followed by a larger project to equip all Corporate Meeting Rooms and Committee Rooms with high quality AV equipment to enable audio and video conferencing capability.

Microsoft Teams

5. Microsoft Teams was launched across the City Corporation on 11th February and has so far proved popular with departments. In April, the total number of active Teams users has reached 1000 staff and there has been strong demand for training and demonstrations.

6. Microsoft have recently commissioned a report into the 'Total Economic Impact of Microsoft Teams', which highlights some opportunities for the Corporation as part of the Fundamental Review. The key findings of the report were;

   a. Teams can reduce the total number and duration of meetings;
   b. With Teams, companies can reduce many other communication software and hardware solutions;
   c. Online meetings can replace the need for travel and overnight stays;
   d. Information workers can save 4 hours per week from improved collaboration and information sharing;
   e. Improved worker satisfaction, integration and empowerment reduce attrition rates;
   f. Less time is spent switching between applications each day;
   g. Employees who work with outside organisations save time by having a shared workspace.

Sam Collins
Head of Change and Engagement, IT Division
T: 020 7332 1504
E: sam.collins@cityoflondon.gov.uk

Agenda Item 8

Committee(s)	Dated:
Digital Services Sub Committee	30th May 2019
Subject: City of London Corporation Information Management Executive Summary	**Public**
Report of: The Chamberlain	**For Information**
Report authors: Sean Green – IT Director	

Summary

Following the presentation of the Information Management (IM) Strategy in December 2018, Summit requested that an IM Executive Summary should be developed that explained the benefits and principles removing any specialist terms.

It is accepted that IM is not in a good state at the City of London Corporation (CoLC). For example, we keep information for too long in silos that makes it more difficult to find the information we need easily and costs money in storing information for longer than is required or useful.

IM is a whole organisation responsibility with IT, HR, Corporate Strategy and Performance and Comptrollers have a lead function in enabling the achievement of the IM Strategy in the organisation.

In the current climate of financial constraint and the fundamental review the pace of delivering the IM strategy may need to be reviewed later in the year.

The strategy is summarised by the following key principles:

- Information acquired by any part of the City Corporation becomes an asset for all the organisation;
- Information is stored securely once and kept up to date while needed and safely disposed of afterward;
- We share information appropriately across the organisation, with partners and with the public;
- Authorised people have easy access to information and to the tools and skills to get the most out of it;
- We promote the culture and leadership needed to look after, share and use information wisely.

This paper provides Members of this Committee with the Executive Summary version of the Strategy agreed by Summit in March 2019 (See Appendix A – IM Strategy Executive Summary attached).

Recommendation(s)

Members are asked to:

- Note the IM Executive Summary

Main Report

Background

1. In October of 2017 Summit agreed the proposal presented to carry out an Information Management (IM) review at CoLC to gain an understanding of the current state of IM strengths and weaknesses for CoLC and provide a roadmap to become a mature IM organisation through completion of an agreed set of deliverables.

2. When the IM Strategy was presented to Summit in December 2019 a request was made that an IM Executive Summary should be produced.

3. The IM Executive Summary is attached as Appendix A.

4. A new Corporate risk associated with the delivery of the IM Strategy was agreed by the Audit and Risk Committee at their May meeting.

IM Definition

5. For the purposes of the IM Strategy, information management is defined as the collection, storage, dissemination/sharing, archiving and destruction of information both electronic and paper. Good information management underpins good information, which in turn underpins good intelligence, which in turn underpins good decision-making.

IM Current State

6. Some of the IM problems identified from a review carried out last year that we need to resolve are:
   - CoLC keeps too much information that we don't really need
   - CoLC keeps too much information in (obscure) silos and struggle to share and reuse it
   - CoLC has poor quality of information, including lack of consistency, unnecessary duplication, out-of-date information and large amounts of unstructured data, resulting in no "single version of the truth" and no "one source" for each data set
   - CoLC focuses on management information and performance reporting rather than analysis and performance improvement. "Hindsight".

7. This has negative impacts on the CoLC, its departments and individual staff and customers:
   - cost – of storage, both electronic and physical

- quality – of decisions and actions based on incomplete or out-of-date information
- time – of people spent looking for the information they need
- risk – of information breaches leading to regulatory sanctions and bad publicity. We also risk losing valuable information that is poorly organised when staff leave our organisation.

Information Management Strategy Summary

8. We want to be in a position where the right people have the right access to the right information, in the right way, for the right reason at the right time.

9. This strategy is not just about compliance with legislation. The main driver behind this strategy is the realising of the value of our information and data estate. To this end, we will ensure that we create and collect the right information for the right purpose and reuse that asset where possible.

10. The information needs to be of high quality, correct, complete, reliable, up to date and accessible and we will put in place and develop the relevant skills, tools and behaviours to make sure this is achieved.

.

Delivering the IM Change

11. No single team can achieve the vision set out in this strategy alone. We all need to have a commitment to improving information management and the use of information in CoLC, working together and learning from areas of good practice and innovation from within both the private and public sectors.

12. To be successful in delivering outcomes and priorities detailed in the IM Strategy there are many different strands which will have different leading service areas:
    - IT for infrastructure, tools and engagement;
    - HR for training and behaviours;
    - Corporate Strategy and Performance for data use and change management;
    - Comptrollers for compliance with information management legislation.

13. Strong governance and oversight are needed if we are to land the positive changes outlined in the strategy and avoid continued replication of the current state. This will be provided by the Digital Task and Finish Group and the Information Governance Group.

14. We will measure our progress towards the vision through a set of activity and performance measures; as well as through softer measures derived from surveys and interviews.

15. We will develop a plan to deliver the IM Strategy and mitigate the actions detailed in the IM Corporate risk.

Corporate & Strategic Implications

16. This strategy will be a key driver behind Corporate Plan outcome 10 'We inspire enterprise, excellence, creativity and collaboration' and outcome 9 'We are digitally and physically well-connected and responsive' whilst also contributing to outcomes 1,2,3,4,8,12.

Financial Implications

17. The capital investment funding to deliver and IM programme will be considered via the Medium-Term Financial Strategy and in year projects through bids for Transformation funds. It estimated capital funding in the order of £2-3m will be required to deliver a 4-year roadmap of IM improvements. If funding is not available there are some incremental changes the organisation can make in the areas of culture, skills and the use of shared drives; however, the changes will be incremental rather than transformational to the organisation.

Conclusion

18. Improving information management practices should be a key focus for CoLC as it is for most organisations, across both the public and private sectors.

19. This is driven by a range of factors, including a need to improve the efficiency of business processes, the demands of compliance regulations (General Data Protection Regulations) and the opportunities for better decision making with better quality, easy to consume and timely information.

Sean Green
IT Director
Chamberlain's Department

E: Sean.Green@cityoflondon.gov.uk

Appendices

Appendix A - IM Strategy Executive Summary

Appendix A - Information Management Strategy - Executive Summary 2018-23

What is information management?

Information management is the formalised collection, storage, analysis, use, sharing and disposal of all types of information, from data through to knowledge.

This can mean gathering, creating, filtering and disseminating information, using it to support decisions and actions, or conserving or disposing of it.

Recent research across the City of London Corporation shows that the way in which information is managed varies significantly. Poor information management incurs significant costs in terms of ill-informed decision-making, missed opportunities and missed threats. Even where the right information is used properly, there is often effort and delay in obtaining and verifying it.

Why information management matters

The more we know and understand, the better we can decide and act, particularly for our stakeholders. Improper gathering, disseminating and analysing of information can put those people at risk. That's why data protection legislation has been passed to regulate this, with stiff penalties for contraventions.

Good information management provides benefits across the City Corporation and for our stakeholders. Its principles are relatively straightforward, but its implementation is made complex by the breadth and depth of its applicability and interdependencies. This is why a strategic approach is required, as set out in the City Corporation's Information Management Strategy Principles (Appendix 1).

How good information management help us

Good information management improves all aspects of designing and delivering services to our stakeholders, but particularly:

- Identifying and measuring service need – what is the problem and how widespread is it?
- Determining service options – what can be done to solve/mitigate the problem, what is the best service solution?
- Designing services for efficiency and effectiveness – making services easier to understand and navigate; encouraging service uptake; minimising blockages and delays; minimising rework;
- Service performance management – is the service working as intended? what are the right performance measures? what can be improved?
- Joined-up approach – what other services might a recipient need and how can these be best co-ordinated?

- Working with partners – getting them the right information; measuring their performance;
- Identifying who isn't being served – identifying gaps in offerings and uptake.

Below are some examples of good information management in action:

- Tell us once – by using information gathered and verified already;
- Pre-filling information on forms - saves customers time and gives them the opportunity to update it;
- Identifying multiple occupancy in a supposedly single-person home;
- Improving property and asset utilisation - so spare capacity can be put to good use or disposed of;
- Improving preventative maintenance - recognising the most effective/ efficient type and timing of maintenance for assets;
- Reducing homelessness - identifying early those people at risk;
- Identifying children at risk early - allowing less intrusive interventions and preventing issues escalating to care orders;
- Better managing shipping of animals across borders - easing reuse of information for high-volume shippers;
- Increasing revenue from visitors to Tower Bridge, Barbican and Monument through acceptable cross-selling based on allowed analysis of visitor and demographic data.

The next steps (See Appendix 2 and 2a)

Technical: Implement the required information management infrastructure.

Policy and skills: Implement skills training for improved information and data literacy, identifying champions in each department/team.

Culture and ways of working: Work with Senior Officers to see how objectives can be translated to departmental business plans and individual's objectives.

Maximise the benefit: Using central analytical resources and working with departments on requirements and priorities where this can be of benefit e.g. preventative measures, saving money, and making better informed decisions.

In summary

The key to information management success is making it an intrinsic and beneficial part of everyday behaviour, rather than treating it as an afterthought or overhead.

The City Corporation will use the principles above alongside recognised good practice standards to develop policies, processes, technologies and leadership that support and encourage the behaviours we need. The built-in continual improvement ethos will ensure that these keep pace with changing business needs.

Appendix 1 - What good information management entails

The right people have the right access to the right information, in the right way and for the right reason at the right time.

To achieves this will need a combination of the right culture, tools and processes, guided by five key information management principles that have been defined for the City of London Corporation:

- **Information acquired by any part of the City Corporation becomes an asset for all of the organisation**
  Information will be open, transparent and available across the organisation. Our staff are custodians of our information assets. We only restrict information for legal, commercial or privacy reasons.
- **Information is stored securely once and kept up-to-date while needed and safely disposed of afterward**
  We will educate, encourage and enable staff to store a single version of information that can be added to and amended. We will discourage duplication and encourage information reuse and repurposing. We will insist on safe disposal of information when no longer needed.
- **We share information appropriately across the organisation, with partners and with the public**
  We will enable staff to easily share our information by developing common standards and processes.
- **Authorised people have easy access to information and to the tools and skills to get the most out of it**
  We will provide the information required – securely, quickly, easily, accurately, conveniently, consistently, and transparently. Systems will be procured, designed and developed to enable effective information sharing, analysis and presentation.
- **We promote the culture and leadership needed to look after, share and use information wisely**
  We will develop and nurture new information management values and behaviours, including a drive to continually improve based on experience and research. We will encourage an approach of curiosity and challenge in the use of our information. Departments will be given the skills and capability to lead and champion this ambition.

Appendix 2 – High Level Activities Plan

IM Outcome 1: CoL has the necessary awareness, tools, skills and culture to promote a set of behaviours and values which understands and manages good information management practice.

CP Outcome 4: Communities are cohesive and have the facilities they need.

These activities focus on developing the values, behaviours and culture we need to deliver good information management. Each activity shows what we need to achieve if the change is to be long lasting and positively landed.

This is based on the ADKAR model[1]:

- **A**wareness of the need for change
- **D**esire to support the change
- **K**nowledge of how to change
- **A**bility to demonstrate skills and behaviours
- **R**einforcement to make the change stick

Activities:

Activity Number	Goals and outcomes of successful change	Activity
1.01	Awareness	Research best practice across the private and public sectors – and benchmark against the performance of organisations providing similar functions.
1.02	Awareness	Introduce a tool to check and monitor compliance with GDPR, mapping information flows across CoL and to external stakeholders.
1.03	Awareness / Desire	Promote the importance and benefits of good information management to Chief Officers and Senior Leadership Teams. Identify data owners across the organisation who will be responsible for the quality, management and use of data.
1.04	Desire	Develop prototype analyses and self-service dashboards to show the "art of the possible" to service managers and Chief Officers.
1.05	Knowledge	Existing support offers for these tools to be refocused on "when" and "why" to use the tools rather than just "how" to use them.
1.06	Knowledge	Develop a training offer across CoL – identify gaps in knowledge and skills and develop a training plan for staff and Chief Officers.
1.07	Ability	Widen the adoption of the tools required for collaboration, with a focus on existing Office 365 tools

[1] https://www.prosci.com/adkar/adkar-model

Activity Number	Goals and outcomes of successful change	Activity
		such as Sharepoint and Teams, reducing volumes of information stored on unstructured H ad W drives, duplication, collaboration via email and time spent looking for information. Widen the use of Power BI to develop self-service capabilities.
1.08	Ability	Provide detailed training, guidance and ongoing support for all staff in the use of information management tools.
1.09	Reinforcement	Identify champions or super users across Information Management disciplines from within existing services. Develop a “community of interest” where officers can discuss problems, share and develop skills and solutions; as well as develop solutions to problems.
1.10	Reinforcement	Determine the change management resources and requirements, ongoing support and training needed to positively land the strategy.

IM Outcome 2: CoL’s information estate is safe, relevant, accurate, reliable, used and trusted.

CP Outcome 12: Our spaces are secure, resilient and well-maintained.

These activities focus on the information lifecycle stages -

Activities:

Activity Number	Information Lifecycle Stage	Activity
2.01	Initiate	Design and build an information asset register for CoL and implement a security classification approach. Define access permissions and retention criteria for our information.
2.02	Initiate	Develop an approach where analytical products identify intelligence gaps which inform future application development.
2.03	Initiate	Form Digital Services Steering Board to oversee and prioritise the business intelligence project pipeline; considering both ethics and statutory compliance.
2.04	Populate	Implement information classification tools across CoL and develop a search facility of our information asset.
2.05	Retain	Identify data and information owners across CoL, and support and train them in their roles and responsibilities. Complete annual information asset audit.
2.06	Retain	Complete migration of unstructured data
2.07	Maintain	Develop a single source of information; including an integration layer of our data sources. This will include

Activity Number	Information Lifecycle Stage	Activity
		transforming and standardising our data to ensure it is amenable for analysis.
2.08	Maintain	Ensure all staff have completed Data Protection training. Implement information tracking tool to identify flows of information throughout the CoL and beyond.
2.09	Maintain	Implement Annual Data Protection compliance audit, and best practice in terms of information management and sharing.
2.10	Maintain	Develop information security function for CoL.
2.11	Share	Develop communications plan about information sharing. Develop Corporate Register of Information Sharing Protocols and agreements (with owners and review dates).
2.12	Share	Develop protocols and mechanisms to receive (and share) data with external parties.
2.13	Dispose	Review and revise information disposal policies and identify safe routes for this to happen.
2.14	Dispose	Develop a consistent approach to records management across the Corporation and develop tools to identify information that can be safely disposed of.

IM Outcome 3: CoL derives real value and benefits from the use of information, data, analysis and modelling.

CP Outcome 7: We are a global hub for innovation in financial and professional services, commerce and culture.

The activities in this outcome focus around the exploitation and *use* of data and using innovative tools and techniques to drive value, open collaboration and innovation.

Activities:

Activity Number	Activity
3.01	Put tools in place to automate manual data processes, improving efficiency and productivity.
3.02	Widen the roll out of self-service visualisation tools across the Corporation. Develop dashboards and analyses for services and support them in their use.
3.03	Develop a pipeline of dashboards and analytical products to be developed. Identify the benefits of each project.
3.04	Develop an approach to prioritisation of analytical projects to be overseen by the Digital Services Steering Board.
3.05	Develop an approach to benefits realisation and monitoring. Identify potential secondary benefits of projects.

Activity Number	Activity
3.06	Develop problem articulation skills across the Corporation (business requirements) – This will help the culture shift from performance to intelligence with a focus on a culture of enquiry and asking "why?" Problem solving needs to focus on the underlying condition not the presenting symptoms.
3.07	Develop prototypes illustrating how advanced analytics such as prediction, prescription and system modelling can drive improvements, realise benefits and improve service delivery.
3.08	Form an analyst network to reinforce the change, develop and share skills, collaborate and innovate.

IM Outcome 4: CoL has sufficient checks, balances and oversight to ensure the successful implementation of this strategy.

CP Outcome 5: Businesses are trusted and socially and environmentally responsible.

The focus of activities in this outcome centre around compliance, assurance and monitoring. The programme needs to have effective governance and oversight mechanisms in place if we are to positively land the change required and reinforce it to make sure continual improvements are made.

Activities:

Activity Number	Activity
4.01	Ongoing programme of consolidating applications and reducing the fragmentation of our data and information.
4.02	Programme of identifying legacy systems which require renewal and upgrades, assessing options for integration with existing systems or procurement of new solutions.
4.03	Identification of organically grown spreadsheets and databases within services – and develop a programme of incorporation in to main applications. Ad hoc systems to be disposed of.
4.04	Development of an ongoing mechanism to catalogue and manage our information asset, identifying data owners and applying security classifications where relevant. Provide a mechanism to search through the asset.
4.05	Ensure that procurement is informed, and where necessary enforced by the IT and Information Management strategies – ensuring compliance with general direction, data standards, security and sharing protocols.
4.06	The Information Management Board will develop a CoL wide register of all Information Sharing Agreements and Protocols, identifying owners and review dates; and oversee the development of any new sharing mechanisms.
4.07	Develop a standard approach to the development of information sharing protocols and agreements between CoL and external partners.

4.08	Develop a mechanism to review what information and datasets can be openly (publicly) published over and above the existing requirements of the Transparency Code.
4.09	Create a Digital Services Steering Board to prioritise and oversee the development of the analytical capability, ensuring that benefits are realised, compliance, and coherence of all related strategies and policies; as well as the implementation of the Information Management Strategy.
4.10	Inform wider procurement - ensure that our contractors comply with our standards, policies and strategies; and ensure that we have direct access to performance and activity data and information about that provision – clauses in contracts (including exit provision).

Committee(s)	**Dated:**
Digital Services Sub-Committee – For Information	**30th May 2019**
Subject: IT Division – IT Service Delivery Summary	**Public**
Report of: The Chamberlain	**For Information**
Report authors: Matt Gosden – Deputy IT Director Eugene O'Driscoll, Agilisys Service Director	

Summary

The overall service performance was good during the period with good levels of satisfaction being reported.

There was a total of 13 incidents for the City of London Corporation and City of London Police in March. This is higher than usual, although 9 of these were caused by external factors such as supplier failures outside of the direct control of the IT service.

Response and resolution times were within expected timelines for most incidents, with the exception of the telephony controller failure, the Tower Bridge network and the Mosaic issue, which each required extensive work from the 3rd parties to resolve.

Problem records have been created where appropriate to identify root causes and to manage improvements.

- There were **2** P1 incidents for City of London Corporation and **2** for City of London Police.

- There were **6** P2 incidents for the City of London Corporation and **3** for City of London Police.

- The Net Promoter Score average for the City of London Corporation/City of London Police for the last 3 months is **69.67**. Any score over **50** is considered very good.

- **90%** of users who completed the customer satisfaction survey following contact with the City of London Service Desk reported a good or very good experience.

- **100%** of users reported a good or very good experience of the City of London Police Service Desk.

PSN accreditation sign off has been completed for the City of London Corporation for another 12 months. This is the end of result of 6 months of remediation work following the IT health check and penetration testing provided by an independent consultancy last year

Recommendations

Members are asked to note this report

Main Report

Service levels and exceptions

City of London Police (CoLP)

1. **P1 incidents**

There were 2 P1 incidents

Affected Service	Reason	Resolution	Problem Management plan
Niche	Niche change to move to new infrastructure.	Change was reverted by Lincolnshire Police (3rd party supplier).	None required
GYE Network	The secondary Clearpass server stopped computers from authenticating because of a certificate error.	All traffic was pointed via the switches to the primary Clearpass server until the certificate error was cleared.	None required

2. **P2 Incidents**

There were 3 P2 incidents

Affected Service	Reason	Resolution	Problem Management plan
Telephony	Vodafone accidentally performed a premature soft cease of the circuit, having agreed to postpone cessation until 31st May.	Vodafone reconnected the circuit.	None required
ASC Call recorder	AC power supply failure.	The server was failed-over to use its secondary power supply; the faulty power supply was replaced.	Problem record created.
Telephony	The Mitel 3300 telephony controller was unresponsive.	The Mitel 3300 controller was restarted.	Project underway to transfer to new technology

3. P1 incidents

There were 2 P1 incidents

Affected Service	Reason	Resolution	Problem Management plan
Mosaic	Incorrect settings on the supplier's network equipment did not match the local environment.	Firewall timeout values were changed at both ends of the connection. This issue is unlikely to recur.	None required
City of London public website	Monitoring detected a significant increase in suspicious traffic to the City of London public website.	Once verified that the source of the traffic was unknown and unauthorised, the source was blocked. A Problem record has been raised to identify opportunities to identify and repel attacks earlier.	Problem record created.

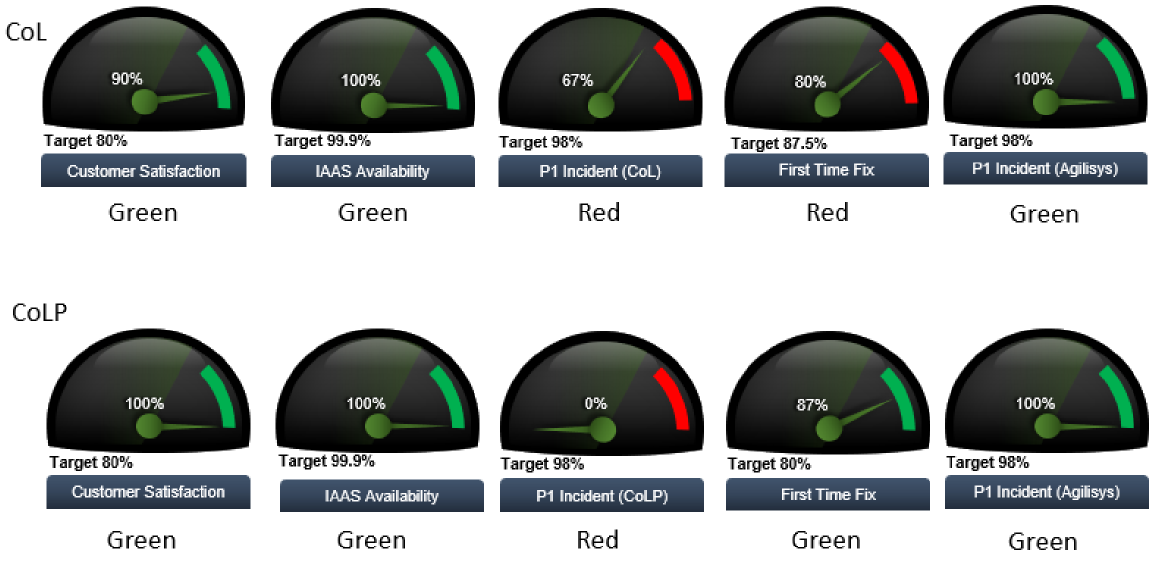
4. P2 Incidents

There were 6 P2 incidents

Affected Service	Reason	Resolution	Problem Management plan
Guildhall 5th floor network	A failed UPS device caused a loss of connectivity for users on the 5th floor of Guildhall	The UPS was removed from service.	None required
Telephony	22 numbers in the West Wing were unavailable when a telephony controller failed.	The telephony controller was rebuilt by the supplier. This issue is unlikely to recur.	Project underway to transfer to new technology
Tower Bridge network	A BT line fault caused a loss of connectivity for users in Tower Bridge	Line fault was repaired by BT	None required
Internet access	Some users were unable to access the internet.	IIS reset on the PAC file server restored service. A Problem record has been raised to identify opportunities to identify a root cause.	Problem record created.
Pubnet	Pubnet was unavailable in Guildhall and City Libraries	Resolved by Tekpool. A Problem record has been raised to manage improvements in the 3rd party service.	Problem record created.
Telephony	There was static noise on Guildhall Art Gallery lines.	Re-seated fibre connections. This issue is unlikely to recur.	None required

5. **Service performance summary is detailed in the dashboard below.**

Gauges to monitor performance – March 2019



Service improvements

6. Police Improvements include:

- Improvements have been made to Solarwinds monitoring tool to reduce and refine alerting.
- Contacts have been reviewed and revised to ensure that support staff have the correct authorisation to log calls with key 3rd party suppliers.
- A review is underway of the critical applications list to ensure that the list meets support for essential applications and services is current.

7. Corporation improvements include:

- London Councils began its migration of servers to IaaS where they will benefit from a more secure and stable environment.
- A change freeze was implemented to successfully support teams working on intensive year-end financial processes.
- Very low number of user escalations, just **1.9%** of open Service Desk contacts were escalated by users.
- Agilisys ISO27001 Information Security Management System reaccreditation audit took place 23rd & 24th April 2019.

8. Customer Satisfaction

- End users in City of London and City of London Police consistently report a very high level of satisfaction when they contact the Agilisys Service Desk, exceeding industry best practice and greatly exceeding local government averages.

- A benchmark of Agilisys customers show the City of London Corporation and City of London Police reporting amongst the highest levels of customer satisfaction when compared to other Agilisys Customers.

PSN Update

9. The City of London Corporation has now received it's PSN accreditation for another 12 months following remediation of required health-check issues and our plan for resolving two outstanding issues by June 19.

Matt Gosden
Deputy IT Director
T: 07714 746996
E: Matt.Gosden@cityoflondon.gov.uk

Eugene O'Driscoll
Client Director – Agilisys
T: 07557 150020
E: Eugene.O'Driscoll@cityoflondon.gov.uk

This page is intentionally left blank

Committee(s)	**Dated:**
Digital Services Sub Committee – For Information	30th May 2019
Subject: IT Division Risk Update	**Public**
Report of: The Chamberlain	**For Information**
Report author: Samantha Kay – IT Business Manager	

Summary

All IT Risks are now in the Risk Management System, with actions included, for the ongoing improvement and continuing assessment to the Management of Risk within the IT Division. The IT Division currently holds 5 risks, a reduction of four from the previous period. There are currently no RED risks. There are no extreme impact risks, there are 4 major impact, 1 serious impact and no Minor impact risks.

IT currently holds 2 risks on the Corporate Risk Register, whilst feeding in to the GDPR Corporate risk which is owned by Comptrollers.

Summary of the Corporate Risks

CR 16 – Information Security - Will continue to be monitored at Corporate level and reviewed for decision at DSSC and Audit & Risk Management Committee in July.

CR 25 – GDPR Regulation Compliance – Will continue to be monitored following the closure of the formal project. It is expected that this will be de-escalated from the Corporate Risk register on the assumption that the internal audit review does not flag any issues of serious concern.

CR 29 – Information Management – Approved by Audit & Risk Committee to be managed as a Corporate Risk.

Recommendation(s)

Members are asked to:
- Note the report.

Main Report

Background

1. Risk remains a key focus for the IT Division and we are continuing to ensure that it drives the priority for project works and Change Management decisions. Regular reviews will ensure the ongoing successful management of these risks across the division

Current Position

2. The IT Division Currently holds 2 Amber risks on the Corporate Risk Register and assists to mitigate one other Amber Corporate Risk. The IT Division currently holds 5 risks, none of which are scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

Current status

3. Since the last report the IT Risk Register has seen the following activity:

   - 2 Risk has been upgraded to Corporate level.
   - 2 Risks have been reduced from Departmental to Divisional level.
   - 1 Risk has been deactivated
   - 3 Risks reduced in score

   The remainder are static and continue to be monitored alongside the relevant on-going projects.

Movement of Risks

4. **Movement from Departmental to Corporate**
   - **CR16 Information Security** – Will continue to be monitored at Corporate level, with a review at DSSC and A&RMC in July.
   - **CR29 Information Management** – Approved by Audit & Risk Committee to be managed as a Corporate Risk. The focus will be to deliver the IM Strategy through a series of actions that are documented in the risk system. (See Appendix A for the details of this risk).

5. **Risks reduced from Departmental to Divisional Level**

   The following risks have been reduced to division level due to mitigating actions being completed, and processes implemented to maintain systems going forward.

   - **CHB IT 001 Resilience - Power and infrastructure**–An ongoing project has started to audit all requirements and make recommendations.
   - **CHB IT 014 Software Lifecycle Mgt –** Following improvements in processes, application rationalisation & more detailed service reviews.

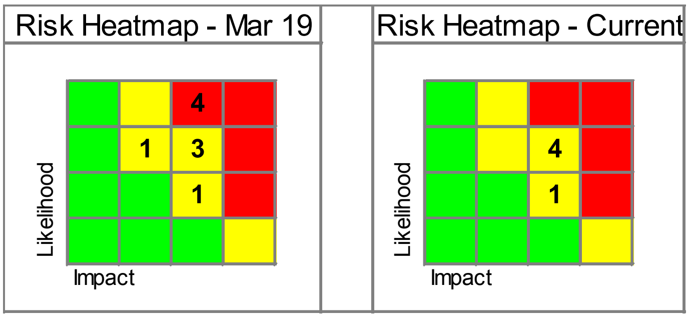
6. Risks that have been deactivated

- **CHB IT 028 IP Telephony and Call recording - Funding Requirements** – Funding for project has been provisioned thus mitigating this risk.

7. Risks that have reduced in score

- **CHB IT 026 Failure to commence CoLP IT Modernisation** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme.
- **CHB IT 027 IP Telephony and Call recording** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme.
- **CHB IT 029 2020 Contract Planning and Procurement Funding** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme
- **CHB IT 020 PSN Compliance –** Following remedial actions the Corporation have been granted the PSN Compliance Certificate for a further year.

The current headline figures for the identified risks in the Division are:



Risk Heatmap - Mar 19

🟩	🟨	🟥 4	🟥
🟩	🟨 1	🟨 3	🟥
🟩	🟩	🟨 1	🟥
🟩	🟩	🟩	🟨

Risk Heatmap - Current

🟩	🟨	🟥	🟥
🟩	🟨	🟨 4	🟥
🟩	🟩	🟨 1	🟥
🟩	🟩	🟩	🟨

8. Further breakdown of current Division risks:

Major Impact:

Risks with “likely” likelihood and “major” impact:	0	⬇
Risks with “possible” likelihood and “major” impact:	3	⬌
Risks with “Unlikely” likelihood and “major” impact:	1	⬌

Serious Impact:

Risks with “likely” likelihood and “serious” impact:	0	⬌
Risks with “possible” likelihood and “serious” impact:	0	⬇
Risks with “unlikely” likelihood and “serious” impact:	1	⬆

⬆ Increase in No.
⬇ Decrease in No.
⬌ Static No.

9. Next steps

- Ensuring that IT deal with Risks in a dynamic manner.

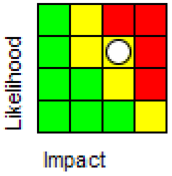
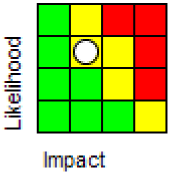
- Ensuring all actions are up to date and allocated to the correct responsible owners.

- Ensuring all members of the IT division including suppliers are aware of how Risk is managed within the Corporation and have a mechanism to highlight areas of concern across the estate.

- IT management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all now reference or identify risk to ensure that Division risks are identified, updated and assessed on an ongoing basis, so the Risk register remains a live system, rather than a periodically updated record.

Samantha Kay
IT Business Manager
E: samantha.kay@cityoflondon.gov.uk
T: 07817 411176

Appendix A – Information Management Risk

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR29 Information Management 08-Apr-2019 Peter Kane	**Cause:** Lack of officer commitment and investment of the right resources into organisational information management systems and culture. **Event:** The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented **Effect:** • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness		**12**	The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. We need to ensure that the IM Strategy is now delivered through a series of actions and activities as detailed below. The actions identified below are Year 1 actions. Actions in subsequent years will be prioritised to ensure full implementation of the strategy. **08 Apr 2019**		**6**	31-Mar-2020	Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR29a	Ensure that CoL has the necessary awareness, tools and, skills to manage information effectively	Work with the Head of Communications to communicate/raise awareness the IM Strategy and Policies. Provide training in SharePoint in preparation for migrating the Shared drives. Implement protective marking and information classification in CoL. Sharepoint to become the Corporate document management solution.	Sean Green	08-Apr-2019	30-Sep-2019
CR29b	Start the culture change by Integrating good information management practice into the Leadership and	HR to work with the IT and the Corporate Strategy and Performance teams to identify the key skills required for good information management. HR to then develop the training to support this.	Chrissie Morgan	08-Apr-2019	31-Mar-2020

	Management stand of the City of London Learning Academy	HR to review where in HR policies and procedures this can be integrated. HR to Work with the senior leadership team to develop a plan and then deliver key messages and communications on the importance, relevance and benefits of good information management.				
CR29c	Ensure that CoL's information estate is safe, relevant, accurate, reliable, used and trusted.	Implement and communicate relevant IM policies and IM Security. Develop and agree a Data Retention policy that links in with departmental retention schedules taking advice from the LMA.	Sean Green	08-Apr-2019	30-Jun-2019
CR29d	Ensure that CoL's derives real value and benefits from the use of information, data, analysis and modelling	IT to deliver the Business Intelligence Infrastructure to ensure that the Corporate Strategy and Performance team have the tools to develop business intelligence reports and analytics to support better decision making across CoL.	Sean Green/Kate Smith	08-Apr-2019	30-Aug-2019
CR29e	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	The Digital Services Task and Finish group to be established to provide governance and assurance that the strategy is being delivered. New IM Policies and compliance are already governed via the IM Governance Board.	Sean Green; Kate Smith	08-Apr-2019	30- May-2019
CR29f	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	Put in place a new Data retention and discovery toolset to ensure we only retain and archive information in line with the agreed policy and retention schedule	Sean Green	08-Apr-2019	30-Nov-2019

Committee(s)	Dated:
Digital Services Sub-Committee	30th May 2019
Subject: IT Division – IT Disaster Recovery Summary	**Public**
Report of: The Chamberlain	**For Information**
Report author: Matt Gosden	

IT Disaster Recovery

Introduction

Business Continuity (BC) and Disaster Recovery (DR) activities are co-ordinated by the Town Clerk's department with initiatives delivered through the Resilience Steering Group - a pan-department group across the City of London and the City of London Police.

As well people and processes, BC and DR activities are often interlinked, and both have a heavy reliance on technology.

This paper provides a brief overview of the IT DR provision, currently in place; supported by the IT Team and their partners.

The paper describes three specific areas:

1. Current approach to Business Continuity and specifically Disaster Recovery plans and activities.
2. An overview of the DR testing which takes place.
3. DR Risks and opportunities.

Recommendations

Members are asked to note this report

Main Report

Current IT DR provision

The cloud, dual sites, resilience and redundancy - what we have in place:

1. Broadly speaking, the Corporation’s data and apps are all hosted in the cloud as part of Office365 and the Agilisys IaaS Datacentres.
2. IT services are provided to the Guildhall through dual resilient BT MPLS WAN links by way of two (active, active; i.e. automated to switch to the alternative link if one fails) routers, to two datacentres, one in Welwyn Garden City and one in Powergate. A DR procedure, as well as the process to invoke a disaster recovery response is in place.
3. Previous tests have been conducted and any errors or failings have been documented and plans improved. The core infrastructure has been upgraded to remove previous single points of failure and diverse links for key connectivity are in place.

Backup as a Service (BaaS)

4. Digital backups taken each evening, with additional backups taken by tape drive and located offsite.
5. Internet service is provided by BT directly to Guildhall and additionally to Powergate, as a resilient backup internet service.

6. Once a DR is invoked, those services that are part of the Resilient IAAS service, will failover to their second location (Welwyn Garden City or Powergate). The remaining services that are part of the Standard IAAS service and located in the location that experiences disruption, will be rebuilt in the second location using hardware acquired at the second location and restored by backups brought across from the Agilisys Hammersmith site.

Testing

IT Disaster Recovery at the Corporation is tested three ways,

7. Annually, through a jointly co-ordinated formal test, based on a given risk profile and a set of “real world” scenarios, that will verify the infrastructure, the business applications being tested and access to them from difference locations using different means.

8. Annually, through a number (19) of smaller regularly scheduled tests, conducted by IAAS, from a list of scenario-led tests of components.

9. Periodically following a major change or upgrade, specific application tests for core or complex applications, such as Oracle. These include application availability and data loss scenarios.

10. It should be noted that although these tests will include shutting down power, services or connections, these are simulated and controlled tests to reduce the impact to the business.

    NB: Business teams are informed that these tests are taking place in advance.

Planned DR tests for 2019/2020

11. The annual DR test is planned for May 2019, to test the following scenarios. Based on a primary risk of loss of power or connectivity to a specific, key local location. (Main Data room in Guildhall).

12. Although the resulting outcomes or technical capabilities during each scenario are generally understood, it is essential that these tests highlight weaknesses in the people, processes and technology. These are subsequently added to a lessons learned process and added to the IT Division risk register or follow up actions where necessary to provide assurance to the Corporation that business will continue in the event of an incident.

13. The May 19 test will include the following:

    - **Power:** Loss of power to the UPS for a key data room in Guildhall, to simulate loss of power to a critical comms room within Guildhall.
    - **Network:** Loss of a link between Guildhall and IAAS – Route will then be via the second link.
    - **Internet:** Loss of internet access between Guildhall and the Internet service being provided by BT – Route will then be via Powergate.
    - **Business Applications:** During the tests, the following business applications will be tested, for login access to the following applications; CBIS, iTrent, Paris and Mosaic.
    - **Connectivity and access to services:** During the tests, the ability to work via Core telephony (Guildhall), via a mobile device or laptop from an external location to verify use of the following Office 365 applications; SharePoint (file store and intranet), Email, Skype, Teams and OneDrive.

DR risks and opportunities

Primary risks:

14. Not all critical business applications are fully resilient end-to-end or supported by architecture that ensures availability or recovery to the degree the business would require.

15. Future major changes and upgrades to the infrastructure, whilst improving the technology, needs business appropriate testing to prove the resilience in the design.

16. The IT DR tests only test a specific set of scenarios, but don't generally include the business to test their processes, responses and third-party providers.

Opportunities:

17. An annual, business led, Business Continuity and Disaster Recovery Test, should be undertaken to test people, process, products and providers, to test the end to end resilient functionality of critical business applications and infrastructure, in the event of a major disruptive event. This should be co-ordinated by the Town Clerk's resilience team with support from relevant corporate functions including IT.

18. Scenario based paper exercises (to reduce cost and disruption) should be conducted frequently, to ensure operational readiness and recovery documentation is always at hand, in the event of a given scenario being realised. These should include non-IT personnel and should be co-ordinated between the Town Clerks Resilience team and IT and their partners.

19. Following the recent work led by the Business Continuity team completing business impact assessments, IT will now follow up to pick up agreement to the opportunities detailed above with Chief Officers.

Matt Gosden
Deputy IT Director
T: 07714 746996
E: Matt.Gosden@cityoflondon.gov.uk

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.

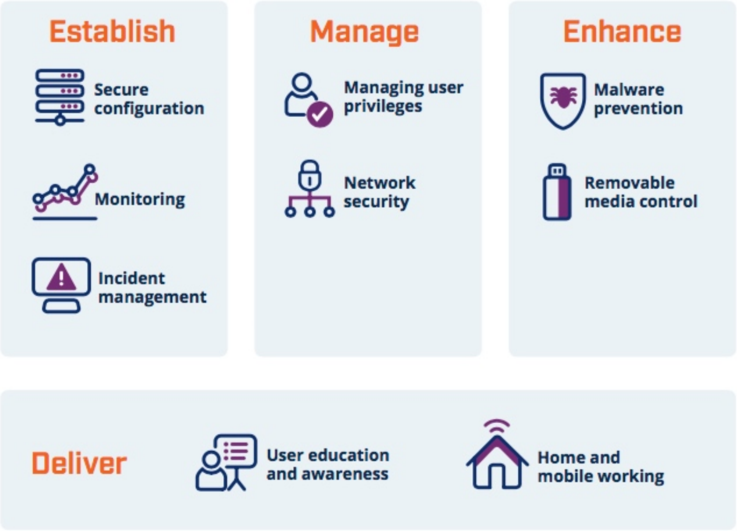
Current Position

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?

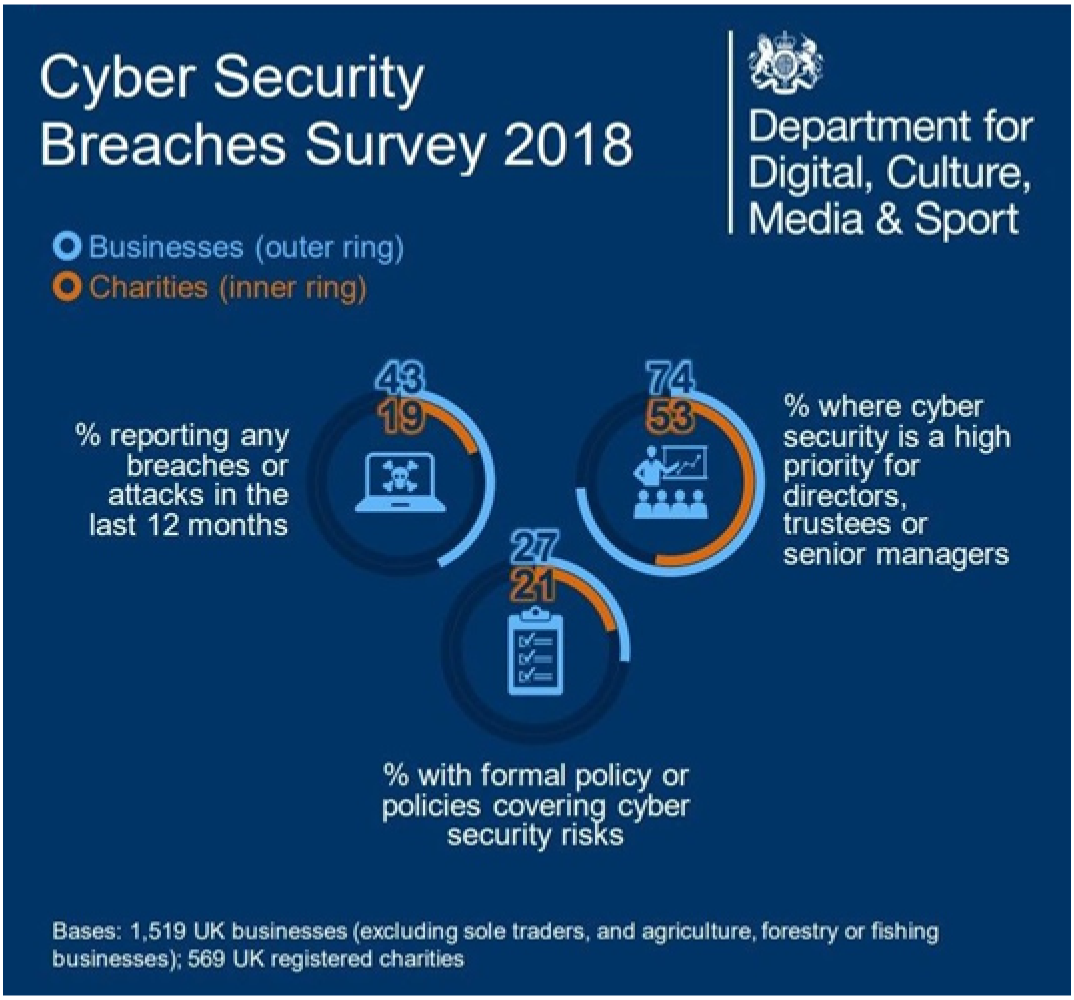
19. A good way to increase our understanding of cyber security is to review examples of how cyber-attacks work, and what actions organisations take to mitigate them.

    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.



Bases: 1,519 UK businesses (excluding sole traders, and agriculture, forestry or fishing businesses); 569 UK registered charities

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:

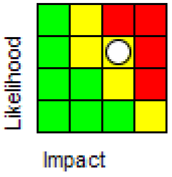
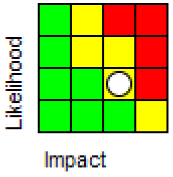
- Appendix 1 – CR16 Information Security
- Appendix 2 – Cyber Security Board Toolkit
- Appendix 3 – Threat Landscape Report

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

Appendix 1 - CR16

Report Author: Paul Dudley
Generated on: 10 May 2019

Rows are sorted by Risk Score

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR16 Information Security (formerly CHB IT 030) 10-May-2019 Peter Kane	**Cause**: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. **Event**: Cybersecurity attack - unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information. **Effect**: Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 2018. Incur a monetary penalty of up to €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.		**12**	A&RMC agreed to add this risk back on to the Corporate Risk register until the July meeting where there will be a full discussion about the status of this risk. **10 May 2019**		**8**	31-Jan-2019	Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR16j	Now in continuous improvement with monitoring and review at the DSSC	New action	Gary Brailsford-Hart	29-Apr-2019	30-Jun-2019

CR16k	Final stages of completing information security projects which will mean that we can assure Members that the City of London Corporation has implemented all the national government recommended security practices and technology achieving a maturity level of 4.	Information Security projects are being delivered as planned. The Information Security team recommended to the Audit and Risk Committee that this risk is reduced to Amber. Move towards a continuous improvement model is being adopted to ensure the controls in place are embedded, mature and reflective of emergent threats and risks.	Gary Brailsford-Hart	29-Apr-2019	30-Apr-2019

This page is intentionally left blank

THE CYBER SECURITY BOARD TOOLKIT[1]

GSC:	OFFICIAL	Version:	1-0
Owner:	Gary Brailsford-Hart Director of Information (CISO)	Date:	May 2019

[1] Content drafted and adapted from the NCSC

Table of Contents

Cyber Security Board Toolkit

About the Board Toolkit

The Board Toolkit is relevant for anyone who is accountable for an organisation in any sector. That could be a Board of Directors, a Board of Governors or a Board of Trustees. Additionally, technical staff and security practitioners may find it a useful summary of NCSC guidance, and can use the questions within the toolkit to frame discussions with the Board.

Scope and structure

Good cyber security is all about managing risks. The process for improving and governing cyber security will be similar to the process we use for other organisational risks. It is a continuous, iterative process and comprises three overlapping components, summarised below:

1. **Get the information we need to make well informed decisions on the risks we face.**
2. **Use this information to understand and prioritise our risks.**
3. **Take steps to manage those risks.**

Crucially in order for these steps to be effective, we need to **get the environment right,** this is broken down into three sections that explain how we do this.

Getting the Environment Right through:

A. Embedding cyber security in the City of London

B. Growing cyber security expertise

C. Developing a positive cyber security culture

Introduction to cyber security for Board members

As a Board member you need to understand enough about cyber security so you can have a fluent conversation with your experts.

What is cyber security?

Cyber Security is the protection of devices, services and networks - and the information on them - from theft or damage via electronic means.

What do I need to know about cyber security?

There are three common myths concerning cyber security. Understanding why they're incorrect will help you understand some key aspects of cyber security.

Myth #1: Cyber is complex, I won't understand it.

Reality: You don't need to be a technical expert to make an informed cyber security decision.

We all make security decisions every day (whether to put the alarm on, for example) without necessarily knowing how the alarm works. Boards regularly make financial or risk decisions without needing to know the details of every account or invoice. The Board should rely on its cyber security experts to provide **insight**, so that **the Board** can make informed decisions about cyber security.

Myth #2: Cyber attacks are sophisticated, I can't do anything to stop them.

Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to the City of London.

The vast majority of attacks are still based upon well-known techniques (such as phishing emails) which can be defended against. Some threats can be very sophisticated, using advanced methods to break into extremely well defended networks, but we normally only see that level of commitment and expertise in attacks by nation states. Most organisations are unlikely to be a target for a sustained effort of this type, and even those that are will find that even the most sophisticated attacker will start with the simplest and cheapest option, so as not to expose their advanced methods.

Myth #3: Cyber attacks are targeted, I'm not at risk.

Reality: Many cyber attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

The majority of cyber attacks are untargeted and opportunistic in nature, with the attacker hoping to take advantage of a weakness (or vulnerability) in a system, without any regard for who that system belongs to. These can be just as damaging as targeted attacks; the impact of WannaCry on global organisations - from shipping to the NHS - being a good example. If you're connected to the internet then you are exposed to this risk. This trend of untargeted attacks is unlikely to change because every organisation - including yours - will have value to an attacker, even if that is simply the money you might pay in a ransomware attack.

How do cyber attacks work?

A good way to increase your understanding of cyber security is to review examples of how cyber attacks work, and what actions organisations take to mitigate them. Reviewing incidents that have occurred within the City of London is a good place to start.

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

The key thing to understand about cyber security defences 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 defences that will help the City of London to combat common cyber attacks. Our section on Implementing effective cyber security measures provides further detail and questions that you can use to understand more about our own organisation's defences.

As a Board member, you will be targeted

Senior executives or stakeholders in organisations are often the target of cyber attack, because of their access to valuable **assets** (usually money and information) and also their **influence** within the organisation.

Attackers may try and directly target our IT accounts, or they may try and impersonate you by using a convincing looking fake email address, click here to see an example. Once they have the ability to impersonate you, a typical next step is to send requests to transfer money that may not follow due process. These attacks are low cost and often successful as they exploit the reluctance of staff to challenge a non-standard request from someone higher up in the organisation.

Good cyber security awareness throughout the City of London, security policies that are fit for purpose and easy reporting processes will all help to mitigate this risk. It is also critical that Board members understand and follow the organisational security policies, so that when an impersonator tries to circumvent them, staff can identify that something is unusual.

You should also consider how information about you that is publicly available could assist an attacker who is trying to impersonate you.

A.

Embedding cyber security into our structure and objectives

Cyber security is not just 'good IT' - it must enable the City of London digital activity to flourish.

Integrate cyber security into the City of London's objectives and risks

There's two reasons why this is so important.

Firstly, cyber security impacts on every aspect of the City of London. Therefore to manage it properly it must be integrated into organisational risk management and decision making. For example:

- Operational risk will likely be underpinned by cyber security because of the reliance on the security of digital services that we use (email services, bespoke software, etc.)
- Some legal risk will be tied in with cyber security risk (such as contractual requirements to protect data or partnerships, regulatory requirements to handle data in particular ways)
- Financial risk is impacted by cyber security (such as money lost through fraud enabled by cyber, revenue lost when services are taken offline by cyber attack)
- Good cyber security will also allow us to take some risk in using new technology to innovate. An overly cautious approach to risk can lead to missed business opportunities or additional (and unnecessary) costs.

Secondly, cyber security needs to be integrated for it to be successful. Good cyber security isn't just about having good technology, it's about people having a good relationship with security, and having the right processes in place across the organisation to manage it.

For example, in order to protect against an attacker accessing sensitive data (whilst ensuring that only those with a current and valid requirement can see it), we will need:

- a good technical solution to storing the data
- appropriate training for staff handling the data
- a process around managing the movement of staff, aligned with access management

Engaging with our experts

Consider whether our reporting structure enables the Board to have the engagement with cyber security that it needs. If the CISO reports to an intermediary to the Board who has a focus on only one aspect - be that finance or legal or technology - this can potentially hinder the ability for the Board to see cyber security's wider implications. In the majority of FTSE350 organisations the CISO now reports directly to the Board.

A good place to start on improving cyber security in the City of London is to consider the communication between experts and members of the Board. Getting the structure right can help, but we also often see a reluctance from both parties to engage, because:

- technical staff think that the Board won't understand them

- the Board think that the technical staff are unable to explain the issues in the context of the strategic aims of the organisation

Improving the communication between these two groups requires effort from both sides:

- **Boards** need a good enough understanding of cyber security that they can understand how cyber security supports their overall organisational objectives

- **technical staff** need to appreciate that communication of cyber risk is a core component of their job, and ensure they understand their role in contributing to the organisation's objectives

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **embedding cyber security into our structure and objectives**.

Q1. As a Board, do we understand how cyber security impacts upon our individual and collective responsibilities?
Q2. As an organisation, who currently has responsibility for cyber security?
Q3. As a Board, how do we assure ourselves that the City of London's cyber security measures are effective?
Q4. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

B.

Growing Cyber Security Expertise

As the demand for cyber security professionals grows, we need to plan ahead to ensure the City of London can draw upon expertise.

Cyber skills are already in high demand, and the Global Information Security Workforce study estimates that by 2022 there will a shortfall of 350,000 appropriately trained and experienced individuals in Europe. Organisations must take steps now to ensure they can draw on cyber security expertise in the future.

Given the lack of suitably skilled individuals and an increasing reliance on digital services that need to be secured, organisations that do not embrace cyber security will soon fall behind.

1. Work out what specific cyber security expertise we need.
2. Establish how urgently we need these skills.
3. Consider how we might recognise professional cyber security skills.

Make the best use of the skills we have

The best way to make use of the skills we have is to identify and focus on the things that are unique to us (or the things that only people within the City of London are most qualified to do). This can be enabled by making use of established, commodity technologies. For example we might choose to allow cloud vendors to build and secure our infrastructure, which frees our experts to spend time exploiting the unique insight they have into our organistion.

Build our best workforce: equal, diverse and inclusive

Due to the cyber security skills shortfall, the City of London must draw and nurture talent from the largest possible pool. The cyber security industry is subject to the same skills challenges as all technology-focused industries. Organisations may find it hard to recruit and retain high-calibre staff from all demographic groups. In fact there are many talented women and minorities working in cyber security, but they are often less visible. They may experience hostile working environments that slow or stop their career, or avoid the industry altogether. Working together to overcome these challenges will give the City of London a competitive edge.

Look beyond technical skills

When designing job roles and desired candidate profiles, particularly at entry level, be imaginative. Protecting the City of London relies on bringing together many different skills, technical and non-technical, to deliver security that aligns with the organisation's objectives. Recruit for broader business skills, aspiration and potential as much as for current technical skills.

Look after our existing talent

When trying to make the City of London more diverse and inclusive, we often focus on bringing in **new** talent, while ignoring the issues that prevent our **current** staff staying and thriving once they are in. The talent available may be beyond our own direct control, but we **can** control how much cyber security talent we lose because of difficult policies and processes, and unwelcoming workplace cultures. As much as strong *security* cultures, we should focus on fully *inclusive* workplace cultures.

Train, buy-in, or develop for the future

Broadly there are 3 options to increase cyber expertise within the City of London.

Train existing staff

Don't just consider the staff who are already in security-related jobs. The NCSC has had huge success training staff from a variety of backgrounds, skills and experience. After all, there are many different aspects to cyber security and someone who is expert at designing a network architecture might have a very different skill set to the person working with staff to make sure security policies are practical and effective.

Depending on the City of London's needs and our staff, training could take the form of on-the-job training, professional qualifications or placements. Do remember that developing cyber security expertise is no different to many other professional areas: staff will require continuous investment, training and development opportunities to hone their expertise and also to keep up with changes in the industry.

- There are many companies who offer cyber security training.
- We could also offer time for study on an NCSC certified degree, or time for a placement on the Industry100 programme.

Buy in expertise

There are several complementary routes available for introducing external expertise. A larger organisation will probably take advantage of all of them.

1. Recruit a skilled non-executive director to the Board.
2. Employ a consultant to provide specific cyber security advice.
3. Identify specific cyber security services which can be fulfilled by a 3rd party.
4. Recruit employees who already have the skills we need.

Recruiting expertise externally can provide a quick solution where there's a lack of specialised cyber security knowledge. However, be sure to identify someone who can adapt cyber security principles to **the City of London**. 'One size fits all' is rarely applicable in terms of cyber security, and someone who just applies an out-of-the-box solution may not be significantly improving our cyber resilience.

Develop future staff: sponsorship, apprenticeships and work experience

Supporting young people to pursue an education in cyber security can be a brilliant way of ensuring a future pipeline of employees with the right skills. There are many schemes aimed at school and university-age students and almost all of them involve some industry participation or support, including apprenticeships, site visits and speaker opportunities.

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **growing cyber security expertise**.

Q1. As an organisation, what cyber expertise do we need, and what do we have?
Q2. As an organisation, what is our plan to develop what we don't have?
Q3. As a Board member, do I have the right level of expertise to be accountable for cyber security decisions?
Q4. As an organisation, are we building an equal, diverse and inclusive workforce to tackle our cyber security skills challenges?

C.

Developing a positive cyber security culture

Board members should lead by example to help promote a healthy cyber security culture.

Establishing and maintaining a healthy culture, in any part of the business, is about putting people at the heart of structures and policies. However, when it comes to cyber security, there is sometimes a tendency to focus almost exclusively on the technical issues and to overlook the needs of people and how they really work.

This rarely results in success. We know, for example, that when official policy makes it hard for someone to do their job, or when a policy is no longer practical, that people find workarounds and ‘unofficial’ ways of carrying out particular tasks.

Without a healthy security culture staff won't engage with cyber security so we won't know about these workarounds or unofficial approaches. So not only will we have an inaccurate picture of the City of London's cyber security, but we will also miss the opportunity for valuable staff input into how policies or processes could be improved.

The board leading by example

They set the tone when it comes to cyber security. Lead by example and champion cyber security within the City of London.

We often hear stories of senior leaders ignoring security policies and processes, or of asking for 'special treatment' in some way (such as requesting a different device to those issued as standard). This tells everyone else in the organisation that perhaps we don't consider the rules fit for purpose, and/or that it is acceptable to try to bypass them.

If policies *don't* work for you as a Board member (that is, if you find yourself doing something different to get our job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it.

Culture takes time and concerted effort to evolve. Don't assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

Putting people at the heart of security

Ultimately, the role of security should be **to enable the City of London to achieve its objectives**. It follows that if our cyber security measures aren't working for people, then our security measures aren't working.

Some organisations fall into the trap of treating people as the 'weak link' when it comes to cyber security. This is a mistake. Effective security means balancing all the different components, not expecting humans always to bend to meet the technology. More importantly, the organisation can't function with people, so staff should be supported so they can get their job done as effectively and securely as possible.

Security and leadership need to make the most of what people's behaviour is telling them. Whilst technical monitoring can look for anomalies, people can act as an early-warning system and intuitively spot something that looks unusual. Ensuring staff know who to report any concerns to can save the organisation a huge amount of time and money in the long run. If staff are working around a set procedure, this may highlight a particular policy or process that needs reviewing.

Develop a 'just culture'

Developing a 'just culture' [1] will enable the organisation to have the best interaction with staff about cyber security. Staff are encouraged to speak up and report concerns, appropriate action is taken and nobody seeks to assign blame. This allows staff to focus on bringing the most benefit to the organisation rather than focusing on protecting themselves.

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **developing a positive cyber security culture**.

Q1. As a Board member, do I lead by example?
Q2. As an organisation, do we have a good security culture?
Q3. As an organisation, what do we do to encourage a good security culture?

1.

Get the information we need to make well informed decisions on the risks we face

Establishing our baseline and identifying what we care about most

Understanding what technical assets we have, and how they're critical to the City of London's objectives, are both key to effective risk management.

There are two tasks in this section, but we examine them side-by-side as the results of one will impact on the other, and vice versa. The two tasks are:

- working out which components of our 'technical estate' (that is, our systems, data, services and networks) are the most critical to the City of London's objectives
- understanding what our technical estate comprises, so that we can establish a baseline which will inform both our risk assessments and the deployment of our defensive measures

Whilst these two tasks have separate purposes, we will need to have some baseline of our technical estate in order to understand which parts of it are mission critical. At the same time, we will need some way to prioritise which areas to baseline, as doing this for our entire technical estate would be a very resource intensive task.

Work out what we care about the most

As with any other business risks, the City of London will not be able to mitigate **all** cyber security risks at **all** times. So the Board will need to communicate key objectives (it might be 'providing a good service to customers and clients', for example) in order for the technical security experts to focus on protecting the things that ensure these objectives are fulfilled.

The Board should also consider what is most valuable to the organisation. For example, the Board might know that a specific partner is crucial to the organisation and that a compromise of their data would be catastrophic. This should be communicated to technical security teams, so that they can prioritise protecting these 'crown jewels'.

It is **critical** that this is an active and ongoing discussion between Boards and their experts:

- Boards will have business insight that security teams may not have (such as which particular partner relationship must be to be prioritised)
- technical teams will have insight into the enablers for key objectives (such as which networks or systems do particular partners rely upon)

Only by bringing these two **together** can we get a full picture of what is important to protect. Once we have this picture it is likely the Board will still need to prioritise within that list. This understanding will not only help focus the aim of our cyber security, but will also inform the assessment of the threat the City of London might be facing.

> **What are our crown jewels?**
>
> Our crown jewels are the things most valuable to the City of London. They could be valuable because we simply couldn't function without them, or because their compromise would cause reputational damage, or it would incur financial loss. Some examples could be:
>
> - bulk personal data
> - corporate systems
> - our public-facing website
> - operational systems

Work out where we are starting from

This provides information that underpins our risk decisions in two ways.

Firstly, it influences the options we have. Knowing which systems are connected to each other, who and what has access to particular data, and who owns which networks are all critical to setting good defences. This information will also be required in an incident to make an assessment of the damage an attacker could be inflicting, or the impact of any remedial actions we might decide to take.

Secondly, it might influence our risk assessment. Sometimes a risk comes not from a threat to an important asset, but from a vulnerability in the City of London's systems. Many incidents are the result of vulnerabilities in older, legacy systems, and the incidents arise not because the vulnerability can't be defended against, but because the organisation didn't have a good enough understanding of their systems to realise they were exposed.

Understanding the **entirety** of our estate can be a daunting, or impossible, task - especially for organisations whose networks and systems have grown organically - but even a basic understanding will help and a good understanding of our priorities can help focus this task.

Identify critical technical assets

Based on the Board's priorities we need to identify what parts of the technical estate are critical to delivering those top-level objectives. This could be systems, data, networks, services or technologies. For example, maintaining a long term customer base may be a priority objective. There are lots of ways that good cyber security could enable this. It could be:

- securing a customer database to protect their data

- ensuring resilience of the order processing system to ensure deliveries go out on time
- ensuring availability of the website so that customers can contact us easily

It can sometimes be difficult to identify these dependencies as they are such an integral part of our operation that they can be taken for granted, but the questions below can help. Doing this in conjunction with baselining our technical estate will also help to potentially identify assets that we weren't even aware of, and are actually critical to providing certain services.

What does good look like?

The following questions should be used to generate productive discussions between the board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **establishing our baseline and identifying what we care about most**.

Q1. As an organisation, do we have a clear understanding of how technical systems, processes or assets are contributing to achieving our objectives?

Q2. As a Board, have we clearly communicated our priority objectives and do we have assurance that those priorities guide our cyber security efforts?

Q3. As an organisation, how do we identify and keep track of systems, data or services that we are responsible for?

Understanding the cyber security threat

Organisations face different types of threat, so each Board's approach to cyber security will vary hugely.

The type of threat faced is shaped by the nature of the organisation and the services an organisation provides. For example, the vast majority of organisations won't be targeted specifically by nation states and so may focus on the threats posed by cyber criminals. However, organisations who form part of, or are providing services to, our Critical National Infrastructure and defence sector may be at risk from nation states.

Understanding the threats faced by the City of London, either in its own right or because of who we work with, will enable us to tailor the City of London's approach to cyber security investment accordingly. We need to consciously make the decision about what threat we are trying to defend against, otherwise we risk trying to defend against everything, and doing so ineffectively.

Get an understanding of the threat

An understanding of the cyber security threat landscape will be key to helping the Board make well-informed governance decisions. For example, we may prepare differently for partnering with a company if we know that they provide important products or services to Critical National Infrastructure and therefore may be a target for a nation state. The Board will already have insight into the threats or challenges facing their sector. This should be complemented by an awareness of the motivations of attackers, and a mechanism for staying up to date with key cyber security developments (for example, the growth of ransomware).

Collaborate on security

One of the best sources of information on good practice and relevant threats can be our sector peers. Attackers often target a number of organisations in the same sector in a similar manner. Cultivating these collaborative relationships on security has two major benefits. Firstly, it can help make our own organisation more resilient, through early warning of threats and improved cyber security practice. Secondly, it helps make the sector as a whole more resilient, which can reduce the appeal to potential attackers.

Cyber Security Information Sharing Portal

The NCSC's Cyber Security Information Sharing Partnership provides a secure forum where companies and government can collaborate on threat information. Access to CISP not only provides the opportunity to securely share intelligence with trusted partners in our sector, but also gives access to sensitive threat reports and the full breadth of NCSC advice.

Assess the threat

Working out the 'threat actors' (the groups or individuals capable of carrying out a cyber attack) relevant to the City of London can help us make decisions on what we are **actively** going to defend against. Whilst investing in a good baseline of cyber security controls will help defend the City of London from the most common threats, implementing effective defences against a more targeted or sustained attack can be costly. So dependent on the likelihood and impact of that threat, we may decide that it is not worth that additional investment.

Ongoing discussion between the Board and experts will help us to prioritise the threats to actively defend against. The experts will have an in-depth understanding of the threat, and the Board will be able to identify the features of the organisation that might make it an attractive target to attackers. It is also critical to have this discussion in advance of any decision that will significantly change the threat profile of the organisation, in order to give technical staff the time to suitably adapt the organisation's cyber security.

> **Working with suppliers and partners**
>
> When assessing the threat, we should consider not only the value that we might have as a standalone organisation, but also the value we may represent as a route into another, possibly larger organisation. For example, we may supply important services to an organisation involved in Critical National Infrastructure, in which case, a nation state may want to attack the City of London in order to access their ultimate target.

Don't underestimate the impact of untargeted attacks

An untargeted attack is where an attacker uses a 'scattergun' approach to reach thousands of potential victims at once, rather than targeting a specific victim. Attackers often use automated, widely available tools that scan public-facing websites for known vulnerabilities. This same tool will then, once a vulnerability has been found, exploit that website automatically, regardless of who it belongs to. This could have just as much impact on the City of London as a targeted attack. A good baseline of basic cyber security controls and processes will protect our system from the majority of these attacks.

Obtain good intelligence - and use it

We will need different types of threat intelligence for different purposes. A good overall threat picture is needed for governance decisions and timely threat intelligence for day-to-day and tactical decisions. Many industry and government partners offer threat intelligence, from annual reports on general trends, right down to highly technical reports on a specific type of malware. We therefore need a mechanism for identifying what intelligence the City of London needs, for what purpose and for sharing that intelligence internally. Critically we then need to **use** that intelligence to inform business decisions, including procurement, outsourcing, training, policy and defence of our networks.

We can also gather threat intelligence internally. We will likely have experience of attacks on our own organisation which can provide strategic insight into activities of threat actors, as well as tactical details on the methods of the threat actors. These specific details will likely come from logging or monitoring within the City of London.

What does good look like?

The following questions should be used to generate productive discussions with the board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **understanding the cyber security threat to the City of London**.

Q1. As an organisation, which threats do we assess are relevant to the City of London, and why?
Q2. As an organisation, how do we stay up to date with the cyber threat?
Q3. As an organisation, how do we use threat intelligence to inform business as usual (BAU)?

2.

Using information to understand and prioritise our risks

Risk management for cyber security

Good risk management will help us make better, more informed decisions about our cyber security.

Most organisations will already be taking steps to assess and manage their cyber security risk. However it is worth considering what the **driver** is for that activity. Often, organisations conduct risk management exercises for 'compliance' reasons, which could include:

- obligations from external pressures (such as regulatory requirements)
- customers' demands
- legal constraints

When done for these reasons, there is a danger of risk management becoming a tick-box exercise. This can lead to organisations believing they have *managed* a risk, when in reality they have merely *complied* with a process which may have (albeit unintended) negative consequences.

Compliance and security are **not** the same thing. They may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices. **Good risk management should go beyond just compliance**. Good risk management should give insight into the health of the City of London and identify opportunities and potential issues.

Integrate cyber security into organisational risk management processes

Many of our organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated with our organisational approach to risk management. Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for us to recognise the wider implications of those cyber security risks, or to consider all the other organisational risks that will have an impact on cyber security.

The role of cyber security should be to *support and enable the business,* and it should do this by managing its risks **without** blocking essential activities, or slowing things down, or making the cost of doing business disproportionately expensive.

Don't make reducing risk levels the measure of success

It can be difficult to measure the success of the City of London's cyber security efforts. A typical output of good cyber security is the absence of a failure, which can be hard to measure, and since cyber security is still a relatively new field there aren't yet many established metrics to draw on.

It is common for risk assessments to deliver some kind of assessment level, be that high medium low, or a number, and so it could be tempting to use this as a performance metric for our cyber security efforts. However, they are a poor metric of our internal security efforts as they are influenced by external factors that are outside of our control - factors which change extremely rapidly. New vulnerabilities are being discovered every day and the number of actors seeking to use cyber means to achieve their aims is increasing.

Driving performance through reduction of a number associated with the cyber security risk will likely incentivise risk assessors and reviewers to underestimate the risks, leading to less informed decisions. Some considerations on what 'good metrics' look like is provided in the “Implementing effective cyber security measures” section of this document.

Be realistic about the risks

Similar 'good practice' risk management principles will apply for managing cyber risk as they would for managing any other organisational risk. However there are two things to bear in mind.

Firstly, solutions and technologies in cyber security are advancing so quickly that it is easy to get caught out using outdated assessments of cyber risks. So we may need to review cyber security risks more regularly than other risks.

Secondly, because cyber security is still a relatively new field, the organisation won't have as intuitive an understanding of cyber security risks, as it might for say, financial risk. As new technologies emerge, there might not be a huge evidence base to draw on to form a risk assessment. This is worth bearing in mind when considering the confidence we have in an assessment of cyber security risk, especially if that assessment is going to be directly compared to assessments of more well-established risks.

A good example of this is cloud security. Many organisations are hesitant to use cloud services because they intuitively assume it is high risk, informed mainly by the belief that storing something valuable with a third party is more risky. In reality, the third party (so in this case a cloud service provider) may have better security measures within their data centres than our own on-site storage. So the *overall risk* may actually be lower. A decision to adopt recent technologies - like cloud storage - would need to be based on a comprehensive understanding of all the risks, rather than an intuitive assessment.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **managing cyber security risk**.

Q1. As an organisation, do we have a process that ensures decision makers are as well informed as possible?

Q2. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

Q3. As an organisation, do we have an effective and appropriate approach to manage cyber risks?

Q4. As a board, have we clearly set out what types of risks we would be willing to take, and those which are unacceptable?

3.

Take steps to manage those risks

Implementing effective cyber security measures

Put in place defences that will protect our critical assets against the biggest threats.

Implementing good cyber security measures is not only a key part of meeting our regulatory requirements but will also help reduce the likelihood of a significant incident. Implementing even very basic cyber security controls will help reduce the chance of an incident.

The Board - Get a little bit technical

Having a basic understanding of cyber security can help us to ask the right questions to seek assurance about the City of London's cyber resilience - just as we would need to have a certain level of understanding of finance to assess the financial health of the City of London. A good place to begin is to discuss our existing cyber security measures with our experts, and the questions below under 'What does good look like?' suggest a starting point for what to ask.

Start with a cyber security baseline

Attackers often use common methods to attack a network. A lot of these methods can be mitigated against by implementing basic cyber security controls. There are several frameworks that outline what good cyber security controls look like. These include the NCSC's 10 Steps to Cyber Security, ISO/IEC 27002 and the NIS Cyber Security Framework.

Tailor our defences to our highest priority risks

The basic cyber security controls will help mitigate against the most common cyber attacks, but once we have that baseline in place, we then need to tailor our defences to mitigate **our** highest priority risks. Our measures will be tailored both to our technical estate (protecting the things we care about the most) and to the threat (protecting against methods used by specific threat actors).

Guidance can help us address these priorities. For example, if we know that one of our critical systems has external connections, we might consider the specialised government guidance on how to safely import data into that system.

Layer our defences

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) help reduce the chances of single point of failure. This approach is commonly referred to as 'defence in depth'.

Each measure provides a layer of security and deployed collectively, greatly reduce the likelihood of a cyber incident. Once we have our cyber security baseline in place we can focus on layering our defences around those things that are most important to us - or particularly valuable to someone else.

Defend against someone inside our network

Defences do not stop at the border of our network. A good defence assumes that an attacker will be able to access our system and works to minimise the harm that they can do once they are inside it. One of the key things we can do to limit the damage they can inflict is to restrict their movement and access. Effectively managing user privileges and segregating our network are common approaches. Identifying an attacker inside our system as soon as possible will also help limit the damage they can do. Monitoring and logging are key to being able to spot any signs of malicious activity.

These measures will also help mitigate the threat from a malicious insider; somebody who has legitimate access to our systems but then uses that access to do harm. This threat ranges in capability and intent, from a disgruntled employee through to corporate espionage.

Review and assess our measures

Good cyber security is a continuous cycle of having the right information, making informed decisions and taking action to reduce the risk. We will need to be continuously assessing and adapting our defences as the needs of the City of London and the profile of the threat changes. To do this it's important to have some way to assess whether our defences are effective.

There are several mechanisms available to technically assess the effectiveness of our security controls. This may include things like testing the security of our networks (pen-testing) through to certification of products or services. We may want to use a combination of internal mechanisms and objective assessment provided by an external source.

Engaging with staff will also help us gain a more accurate picture of the City of London’s defences. It will also give us the opportunity to get valuable staff input into how policies or processes could be improved. Metrics or indicators can also tell us where we need to change our approach or adapt to new circumstances. Understanding exactly what an indicator is telling us may require further investigation of the situation. An example is the trend in people reporting suspicious emails. A decline in the number of people reporting can either mean fewer malicious emails are getting through to people’s inboxes, or it could mean fewer people are reporting any concerns because they don't receive feedback when they do, and therefore believe nothing is ever done afterwards.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing the City of London's cyber security measures**.

Q1. As an organisation, how do we assure ourselves that our measures are effective?

Q2. As an organisation, what measures do we take to minimise the damage an attacker could do inside our network?

Q3. As an organisation, do we implement cyber security controls to defend against the most common attacks?

Collaborating with suppliers and partners

Cyber attacks on our suppliers can be just as damaging as an attack on our own networks.

There are four reasons why cyber security is a key consideration when collaborating with suppliers and partners:

1. We increase the number of routes and external touchpoints in the City of London. So if any of them are compromised, we are also at risk.
2. We may be targeted as a way into the organisation we are supplying.
3. Our suppliers may be targeted as a route into the City of London.
4. We may be sharing sensitive or valuable data or information that we want suppliers to protect.

Being able to demonstrate a good level of cyber security is increasingly a key component of supplier and provider contracts, and is already a requirement for many government contracts.

Build cyber security into every decision

All organisations will have a relationship with at least one other organisation, be that the provider of our email service, or the developers of the accounting software we use, through to our traditional procurement supply chain. Most organisations will be reliant on multiple relationships. Each of these relationships will have a level of trust associated with them, normally some form of access to our systems, networks or data. There are three key things we therefore need to ensure:

1. That this access doesn't provide a route for an attacker to gain access to the City of London, either through deliberate action or unintentional consequence.
2. That any partner or supplier is handling any sensitive data appropriately and securely.
3. That any product or service we buy has the appropriate security built in.

Cyber security risk should be a key consideration in any decision on new relationships or collaborations. This includes decisions on suppliers, providers, mergers, acquisitions and partners.

Identify our full range of suppliers and partners, what security assurances we need from them, and communicate this clearly

Review our current supply chain arrangements to ensure we are setting out our security needs clearly and identifying the actions we need to take as a result. If we ourselves are a supplier, ensure you meet the security requirements set for you by the customer as a minimum.

Ensure that the security requirements we set are justified and proportionate and match the assessed risks to our operations. Also be mindful of the current security status of our suppliers to give them time to make the necessary improvements. It might be useful to include references to the following government guidance that can help to establish a baseline of cyber security:

- 10 Steps to Cyber Security
- Small Business Guidance
- Cyber Essentials

The following government guidance can help **us** to assess our own security needs from suppliers:

- Supply chain guidance
- Cloud services guidance
- Software as a Service guidance

Get assurance

Security should be built into all agreements from the start, and we should have confidence that our security needs are being met. Dependent on our relationship with the supplier or provider and our resources, we could seek assurance of this through testing, auditing or adherence to accreditation standards.

Consider the implications if our supplier is compromised

No matter how comprehensive our security agreements with our partners are, and no matter how well they implement their controls, we should assume that our partners **will** be compromised at some point. We should plan the security of our networks, systems and data accordingly with this assumption in mind. This is also worth considering in our security agreements; what are we expecting of them and their response? Do they have to notify you? Do they have to assist us if we are consequently also compromised?

What does good look like?

The following questions can be used to generate productive discussions with our technical team. The aim is to identify what constitutes 'good'cyber security in terms of **supply chain security**.

Q1. As an organisation, how do we mitigate the risks associated with sharing data and systems with other organisations?
Q2. As an organisation, how do we ensure that cyber security is considered in every business decision?
Q3. As an organisation, are we confident that we are fulfilling our security requirements as a supplier?
Q4. As a Board, do we have a clear strategy for using suppliers, and have we communicated it?

Planning our response to cyber incidents

Good incident management will help reduce the financial and operational impact when they do occur.

Incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. Being prepared to detect and quickly respond to incidents will help to prevent the attacker from inflicting further damage, so reducing the financial and operational impact. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on our reputation.

Ensure we have a plan

1 in 10 organisations don't have an incident management plan. If you're one of these organisations, then we should address this immediately.

Understand your role in incident management

Incidents often occur at inopportune moments and most people's decision making is compromised in times of crisis. For these reasons, **everyone** must have a clear understanding of **their role** and the organisational response in advance, especially Board members who would likely be representing the organisation in the media.

The Board also needs to be explicit about who it is willing to devolve authority to (especially outside core working hours), and exactly what that authority covers. For example, does that cover calling in a contracted incident response company, or taking down a public facing website? The Board also needs to be explicit about when it wants to be informed of an incident, both in terms of at what stage of the incident, and in terms of what significance of incident they need to know about.

Get involved in exercises

The best way to test these processes and thresholds (and to get a good understanding of the Board's role) is through exercising the incident management plan. If we would be involved during a real incident, then we should be involved in an exercise. Doing this in conjunction with operational staff can also help to highlight issues around authority for critical decisions. Even if we do not have a direct role in responding to an incident, running an exercise can be a good way to understand the realities of how an incident would impact on the City of London.

Drive a 'no blame' culture

Post-incident analysis provides insight that can help us reduce the likelihood of incidents occurring in the future and reduce their potential impact. Crucially in order to get this insight we need to be able to be honest and objective about what has happened. This can only happen in a no blame culture, such as we would use when investigating health and safety incidents. Critically for the Board, new regulation, such as GDPR, is clear that responsibility for incidents or data breaches sits with the organisation and not an individual. Therefore the Board is ultimately responsible for any cyber security incident as the governing body. Apportioning blame to a specific individual within the organisation will be treated as poor cyber security practice.

Work out what an incident would look like

One of the most common things overlooked is being able to identify what constitutes an incident. There's two aspects to this:

1. Working out how we would spot an event in the first place.
2. Working out at what point an **event** (something happening on our networks or systems) becomes an **incident**.

How would we spot an event?

Depending on their motives, an attacker is unlikely to tell us when they have successfully compromised the City of London, so we need our own methods to identify an intruder or an attack. This normally takes the form of monitoring. Monitoring refers to observing data or logs collected from our networks or systems to identify patterns or anomalies that could indicate malicious activity. Even if we don't have monitoring to identify the incident, it is still useful to collect system or network logs (especially those relevant to our critical assets) so that we can retrospectively review them once we know an incident has occurred.

When does an event become an incident?

This is often not a clear cut decision. We can try and gather as much information as possible to inform our assessment of an 'event', but we probably won't have a complete picture of what has happened. Beginning an incident response might have implications for cost, reputation and productivity, so we will want to consider who has the authority to make this decision, and what the thresholds are for an incident **in advance**.

What is a cyber security incident?

A breach of the security rules for a system or service - most commonly:

- attempts to gain unauthorised access to a system and/or to data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owner's consent
- malicious disruption and/or denial of service

Use the information we already have

All the information we have previously gathered on what's important to protect, the threat and our technical estate will provide critical insight in two key areas:

- It will give us insight into the impact of incident. If the attacker has accessed a particular user device, what could they access? Could they access those things we care about the most?
- It will help us determine our operational response. If the attacker is on a specific network can we isolate that network? If we can, what would the impact be on the City of London?

Take pre-emptive measures

Put measures in place to help reduce the harm that an attacker could do. This could be:

- introducing measures that restrict their movement once they are inside our network
- pre-emptively reducing the impact of attacks (for example, backing up our data will help to reduce the impact of a ransomware incident)

As with any other defensive measures, these should be focused on protecting what is most important to you.

Make an Incident Management plan

Cyber Incident Response is a complex subject as no two incidents are ever the same. However, as with all business continuity planning, we can develop a plan that will outline the key elements of our response. Our plan should not only cover the technical elements, but also:

- the people and process elements such as media, customer and stakeholder handling
- reporting to regulators
- dealing with legal actions

For more common incidents (such as DDOS) it may be helpful to develop a specific 'playbook' setting out the City of London response.

Test our plan

Rehearsing our response to different scenarios is key to ensuring our plans are effective and remain current. There are various exercising packages we can use. This will be a critical part of the role for any staff involved directly in incident management, but every Board member also needs to understand their specific area of responsibility during an incident.

Learn lessons

An often overlooked aspect of incident management is the post-incident review. An incident can provide valuable insight into our cyber readiness, including:

1. The **threat** the City of London faces.

- Who carried out the attack and was it targeted?
- Did they go about it in the way we expected?
- Did they go after the things we expected?

2. The effectiveness of our **defensive measures**.

- What did our defences protect against?
- What didn't they?
- Could they be improved?

3. The effectiveness of our **incident response measures**.

- What would we have done differently?
- Did our response help to reduce the impact of the incident?
- Did it make some aspects worse?

> **Working with suppliers and partners**
>
> Our plan should also consider how we mitigate the impact on any partners or customer organisations if we were compromised. When do we inform them? What mechanisms are in place to limit the damage it could do to them? We should also consider what we would do in the event that a supplier is compromised; we may not have control over how they deal with the incident. What would we be able to do independently to reduce the impact on the City of London? The best way to mitigate this risk is to have a collaborative approach to our security with our partners and suppliers.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **responding to cyber incidents**.

Q1. As an organisation, do we have an incident management plan and how do we ensure it is effective for cyber incidents?
Q2. As an organisation, do we know where we can go for help in an incident?
Q3. As an organisation, do we learn from incidents and near misses?
Q4. As an organisation, how would we know when an incident occurred?
Q5. As a Board, do we know who leads on an incident and who has the authority to take any decisions?
Q6. As a Board member, do I understand what's required of my role during an incident, and have I had training to equip me for that role?

This page is intentionally left blank

Threat Landscape Report

Executive

Q1 2019

TLP:GREEN

CERT-EU
Computer Emergency Response Team for The EU Institutions, Bodies and Agencies
https://cert.europa.eu

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community,
but not via publicly accessible channels..

Executive Summary

Direct Threats

Targeted attacks	CERT-EU has not observed any targeted intrusion attempt affecting EU institutions, bodies or agencies (EU-I). However, several advanced persistent threat (APT) groups were active in Europe, including Russia-based APT28 and Turla, North Korea-based Lazarus, and Chinese APT10. There was a Twitter hacktivist campaign, calling for disruptive action against the European Parliament (EP) and political parties in protest for the vote and approval of new amendments to the Directive of Copyright in the Single Digital Market. Some hacktivist-related denial of service attacks targeted public websites of EU-I. Some targeted phishing campaigns have impersonated other EU-I, colleagues, and an EU-I IT desk.
Common cyber-threats	There were no ransomware attacks affecting EU-I. Magento (online credit-card skimmer) and Emotet have been the main banking malware targeting EU-I end users. As it has been established over several observation periods, there were again appearances of new general purpose trojans. Limited cryptojacking activities were reported. Common phishing attacks (invoice, personal banking, purchase, shipping, etc.) have continuously affected EU-I. Credential leaks, that is username/password combinations discovered in publicly available repositories, have remained for several quarters the most widespread events identified with at least 39 impacted EU-I. Finally, successful password spraying attacks have been observed.

Broader Threats – Critical Sectors

Transport	Hackers and cyber-terrorists present an ever-evolving threat to air travel, constantly testing for new vulnerabilities, including the possibility that hacked drones could be used to throw planes off course. In the maritime sector, capsizing a ship with a cyberattack is a relatively low-skill undertaking, according to security researchers. In the automotive sector, executives of several EU car manufacturers are upset that GPS systems are vulnerable to attacks and spoofing.
Energy	Energy companies can become victims of severe, opportunistic and disruptive attacks (e.g. a Norwegian aluminium and energy producer was severely affected by ransomware). Energy companies in the US, Ukraine, South Africa and the Middle East were subject to intrusions by hackers of various origins (incl. Russia, Iran and China). Vulnerable electric vehicle charging stations can become an entry point for targeting electric grids.
Health	Health care entities in several countries (Sweden, US, Canada, Singapore and others) became victims of health data breaches mostly due to inadequate security measures or misconfigurations. Attackers may try to monetise these data by offering them for sale in illegal cybercrime markets. Researchers found new medical devices vulnerable to malicious manipulations over their wireless interface.
Banking& Finance	A major cyber heist has been reported in Bank of Valetta. The attack is highly likely related with cybercrime group Empire Monkey. Magecart group 12 accelerates credit card data collection with the use of supply chain infections. Cobalt group remains active with impersonations of credible companies. Ursnif malware evolves and targets some European countries.
Digital infra	Huawei is fighting back the Five Eyes ban on their 5G infrastructure products. BGP and DNS hijacking is still a major problem with several attacks abusing these protocols and services. Russia strives to control domestic access to satellite internet services and rehearses disconnecting from the global internet. Iran is also planning a similar action. Japan plans to proactively scan its citizens' IoT devices for vulnerabilities before the Olympic Games.
Digital services	Facebook is purportedly making an effort to stay ahead of fake news and election targeting on its platforms. On the other hand, it suffered the biggest outage in its history. Russia plans to ban what it deems to be fake news and insults on online platforms. As regards e-commerce, Magecart card skimming campaigns continue to make victims worldwide.
Defence diplomacy	Military and diplomatic entities in Eastern Europe were subject to targeted intrusions attempts from actors with alleged Russian ties. China and North Korea are in all likelihood using cyber-espionage to steal military technology (resp. naval and dual use technology). The US allegedly attempted to sabotage Iran ballistic missile project while Iran claimed to hack US drone operations. US experts helped the United Arab Emirates to spy on diplomats in the Middle East.

Broader Threats - Geopolitical

US	The US charged, sentenced, arrested or disrupted assets of foreign hackers from Iran, China, North Korea and Romania. In the Middle East, the US allegedly attempted to sabotage Iran ballistic missiles project by slipping faulty parts into the supply chain and released a mobile spying tool to the UAE.
China	China deployed artificial intelligence-based security software for citizen surveillance purposes and reinforced legislation to inspect all kinds of networked units. China is suspected to benefit from its dominant position on the digital infrastructure segment (China Telecom rerouting international internet traffic – BGP hijacking – possibly for monitoring purposes, Huawei's involvement in 5G networks and undersea cable networks). Several Chinese groups are involved in cyber-espionage operations. Targets include technology firms in Europe and the US, a business conglomerate in Japan, gaming firms in Asia, naval technology with military applications in the US, Canada, and Southeast Asia.
Russia	Russia reinforces legislation on the independence and resilience of the Russian segment of the internet (RUNET). Russia presses foreign social media and internet search companies to comply with domestic internet control regulations. Russia is suspected of miscellaneous operations in Ukraine (intrusion in the energy sector, interfering into the presidential election, and spying on military) and the EU (e.g. entities dealing with international and security affairs). Facebook removed social media accounts tied to Sputnik for "coordinated inauthentic behaviour."
Iran	Iran removed US technologies from its national internet (NIN) and performed resilience exercises. Iran-based actors allegedly conducted a large DNS hijacking campaign to collect sensitive information on companies and government entities in the Middle East and Europe. Iran-based actors are purportedly conducting espionage operations against the aviation and telecom industry as well as diplomatic entities. Iran is training domestic actors for cyber and information operations while Facebook removed supposedly pro-Iranian accounts.
North Korea	North Korea's Reconnaissance General Bureau (RGB) maintains approximately 200 cyber units outside the country to generate revenue and gather intelligence for the regime. A United Nations panel of experts reported that cyberattacks on financial institutions to illegally transfer funds "have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016". North Korea is suspected to have stolen the personal data of almost 1,000 North Korean defectors via cyber means.

Broader Threats - Motives

Cyber conflicts	Russia is suspected of miscellaneous operations in its neighbouring environment: Ukraine (intrusion in the energy sector, interfering in the presidential election, and spying on military) and in Moldova (information operations). Iran and the US are engaged in cyber-conflict involving various kinds of cyber-operations (sabotage, information operations, hijacking drones).
Espionage	Researchers found an online database that likely contains real-time surveillance data about Chinese Uyghur population. The Israeli NSO group's founder denies the company's involvement in Khashoggi's murder. China is accused of leveraging LinkedIn for spy agent recruitment. Russian lawful interception framework SORM will allow the country to get access to IoT devices and in addition to RUNET, there is plausibly a Russian-only IoT network in the making.
Hacktivism	Political hacktivism was triggered by legislative initiative (EU Copyrights Directive), opposition to a political party (Italy) or protests against a regime (in Venezuela, Algeria, Iran). In the Middle East, hacktivists continue to fight the influence of the Islamic State of Iraq and Syria (ISIS). Nationalist-hacktivist protest against violence on their compatriots (Syria, Lebanon), or entities perceived to be against national interests (Turkey). Hacktivists have employed different techniques, mostly denial of service, defacement, leaks and doxing.

Techniques, Tactics & Procedures

Malware	LockerGoga ransomware targets multiple industries, in likely targeted attacks, and causes great operational and financial damage. Scanbox reconnaissance watering holes are still in use. Russian APT groups develop new tools and redevelop old ones.
Techniques	Several malware, such as SLUB and RogueRobin use publicly available legitimate tools for command and control. Researchers describe ToRPEDO, PIERCER, and IMSI-Cracking attacks against mobile networks. Gmail services can be abused in several ways. ASUS laptops are involved in a massive supply chain attack. Heart defibrillators and smart car alarms are found to be vulnerable to cyber-attacks.
Tactics	Supply chain attacks have become a widely adopted tactic for hackers with different motives (criminals, espionage, sabotage): ASUS live update (espionage by a likely Chinese group), Magecart infecting payment website for card-skimming (cyber-criminals), the US suspected to sabotage Iran missile by slipping faulty parts into the supply chain (sabotage), US-based software provider compromised in a supply chain attack, tablets and smartphones from Polish, Chinese, and Hong Kong manufacturers were found to contain malware-infected firmware.

Selected Attacks

#	Attack	Type
1	A Chinese espionage group dubbed APT40 conducted espionage activities with the specific aim of theft of naval technology with military applications.	Global espionage China
2	A team of former US government intelligence operatives working for the United Arab Emirates hacked into the iPhones of activists, diplomats and rival foreign leaders.	Targeted attack Diplomacy
3	US reportedly attempted to sabotage Iran's ballistic missile and space rocket programs by slipping faulty parts into the supply chain.	Targeted attack US, Iran
4	A Chinese espionage group dubbed APT10 attempted to breach the networks of several European, US and Japanese firms: the Norwegian software firm Visma, HP, IBM and Keidanren conglomerate.	Global espionage China
5	APT28, a highly likely Russian threat actor, targeted an EU member state' civil-law institution dealing with international and security affairs.	Targeted attack Russia
6	Facebook removed hundreds of Russia-initiated accounts for "coordinated inauthentic behavior", including some linked to the state-owned news agency Sputnik.	Social media Russia
7	A DNS hijacking campaign dubbed "DNSpionage" targeted victims across the globe on an almost unprecedented scale, with a high degree of success.	Internet infra Iran
8	LockerGoga ransomware caused significant disruption in several countries (including a US chemical company, a Norwegian industrial firm and a French engineering company).	Malware
9	Between June and November 2018, a sophisticated supply chain attack dubbed ShadowHammer compromised the ASUS Live Update Utility and affected 500 000 computers.	Techniques Supply Chain
10	Bank of Valetta was the victim of a major cyber heist that led to fraudulent international payments totalling 13 million euros.	Bank Cyber-crime

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 16

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Agenda Item 18

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Agenda Item 19a

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank