Cyber Security and Information Governance - Corporate Risk Review

The purpose of this report is to update Committee on the work currently undertaken and planned to help manage the risk associated with Cyber Security and Information Governance.

Introduction

1. Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computer systems.

2. Information management is the collection, storage, dissemination, archiving and destruction of information. It enables teams and stakeholders to use their time, resource and expertise effectively to make decisions and to fulfil their roles.

3. Both are essential to the success of service delivery for the Council. A cyber attack leading to any unscheduled downtime of systems would mean that the Council is unable to deliver services. Whilst failing to manage information correctly could lead to service failure, inefficiencies and risk to the Council reputation.

4. The current risk rating for this likelihood of 4 and impact of 5. There are a number of areas that the Council is working on to reduce the likelihood but the impact of not having systems or losing data would remain a high impact of 5.

5. The General Data Protection Regulation (GDPR) came into being in May 2018. It extends the data rights of individuals, and places a range of new obligations on organisations that process personal data.

Work undertaken/being undertaken to mitigate the risk for Cyber Security

6. Public Sector Network (PSN): The Council achieved compliance with the PSN network security requirements again for 2018/19. The PSN is the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. The compliance process ensures that the Council has the technical design, security, processes and procedures to manage information securely. This also includes an external security test of the network.

7. Cyber Essentials: Following a formal assessment by an external accreditation body, Digital and IT have been awarded the Cyber Essentials Certification. The certification gives peace of mind that defences will protect against the vast majority of common cyber attacks. Digital and IT are currently carrying out a Cyber Essentials Plus gap analysis with external assessors and looking to implement in the future. Cyber Essentials Plus is a more rigorous test of our cyber security systems.

8. Phishing: "the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers." Phishing is one of the biggest risks for the Council and on the internet in general. An inhouse tool has now been developed to assist in raising awareness across the Council for the importance of being aware of the risks of phishing and to ensure that staff are aware of what to look out for to avoid falling for any scam and what to do if concerned.

9. Unsupported Hardware and Software including Operating System. Significant progress has been made to remove unsupported operating systems over the past 12 months to ensure the Council is on supported and maintained versions. This is an ongoing process as other hardware and software will regularly become end of support. There is a programme of work that is continually reviewing and upgrading across the Council.

10. National Cyber Security Centre (NCSC): We have continued to foster our links with the National Cyber Security Centre (NCSC), which is part of GCHQ and are participating in several initiatives with them including:

    a. NCSC Webcheck service, which continually scans our internet facing infrastructure, websites (the ones ending in .gov.uk), firewalls and technical components of web sites for problems and misconfigurations, and alerts us when anything is discovered, this is a good service and thus far we have had little to fix. As a result of this NCSC have asked us to be an alpha test of the new improved service.

    b. Took part in the pilot of the Cyber Security Stocktake of English Councils before the main survey being sent out in August. We have just received the results of this with a overall rating of Amber Green which puts us in the top quartile of English councils, with London as a region doing fairly well overall.

        i. The following areas were of strength for the Council: training and awareness; our information governance and cyber security structures, and onwards in to reporting to senior management. We were also confirmed as inline with the technical controls and expectations within the UK government Minimal Cyber Security Standard (published in summer 2018 this is the emerging standard for the UK public sector)

        ii. There are a number of areas that the Council is working to strengthen: the update of the Digital & IT risk register to include a wider range of cyber security; further training in cyber security; participation in NCSC desktop exercise and embed cyber security into the overall Council Business Continuity Plans, finally better using of logging and reporting from systems and use of threat intelligence

Work undertaken/being undertaken to mitigate the risk for Information Governance

11. The overall aim of Information Governance work for the Council is to protect the data and information that the Council holds about our Residents, Customers and Businesses.

12. The Council has updated policies and processes to ensure that the Council was prepared for the new requirements of GDPR and to ensure that it regularly monitors and reviews these in line with any updates.

13. The Council has reviewed and updated the Information Asset Register and Retention and Disposal Schedule. These registers enable the Council to identify, understand and manage information assets as well as any associated risks. These will be reviewed and updated quarterly.

14. The Council's website has been updated to comply with and reflect the change in legislation and to provide clear guidance on how the public can exercise their data rights. Privacy Notices are displayed on our webpage.

15. Processes have been put in place for the new and existing data rights, these include Subject Access Requests and the Right to Erasure. Staff receive training and guidance on handling these requests.

16. When 'Consent' is the necessary lawful basis for processing information we have worked with teams to ensure that the correct process is being followed. The GDPR sets a high standard for consent, this is documented in our Information Asset Register ensuring that our obligations under Article 7 of the GDPR are met.

17. Data Protection Impact Assessments (DPIA) is a process to help us identify and minimise the data protection risks to a project. The DPIA process has been reviewed and embedded into the project management and commissioning process.

18. Training and awareness for staff and Councillors on Information Governance continues to take place. Those with specific roles such as Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian have had specific training. Throughout the year training and drop in sessions have been provided to all staff.

19. Review and ensure that the commissioning arrangements for any spin out or arms length companies include satisfactory Information Governance and Security requirements and that these are checked on a regular basis.

20. There is a programme of work for 2019/20 to ensure that improvements continue to be made in the management of Information.

Next Steps

21. Forward plans for Information Governance and Digital & IT are developed and maintained to ensure that the Council continually improves Cyber Security and Information Governance for the Council. The plan includes the following:

    a. regularly review and update policies and procedures

    b. Undertake data flow mapping exercise across the Council and link to the Information Asset Register

    c. Continue to represent the Council at the London-wide Information Governance network and work collaboratively where appropriate. Warning, Advice and Reporting Point (WARP's); Information Security for London (ISfL) and Information Governance for London (IGfL).

    d. Review the Digital & IT risk register to include all Cyber risks

    e. Continue to work with NCSC on initiatives such as the tabletop Disaster Recovery /Business Continuity exercise

    f. Involvement in the MHCLG Pathfinder program which seeks to develop better response planning in the event of cyber incidents.

    g. Continue to ensure the technical compliance with requirements for PSN, DWP, NHS etc.

h. Ensure staff are aware of all their responsibilities and embed a culture of Cyber Security and Information Governance into the Council.

i. Councillor and Staff training will continue to be maintained and developed and ensure that we enforce training is completed to reach 100% of the Council.

Author of report - Mark Lumley, Assistant Director, Digital & IT

- None other than those referred to in this report