Report to:	Corporate Scrutiny Committee
Date:	11 March 2022
Subject:	**Cyber Security**
Director:	Angela Taylor, Director, Corporate and Commercial Services
Author:	David Gill, Head of ICT Services

1. Purpose of this report

1.1 To provide the Corporate Scrutiny Committee with details on West Yorkshire Combined Authority's current position regarding cyber security and ICT resilience.

1.1 To set out the current risks and how the Combined Authority will evolve following the reliance on technology and system/information security vulnerability which has been exposed since the pandemic.

2. Information

2.1 In 2018 the Combined Authority commenced delivery of its Corporate Technology Programme. This digital transformation programme enabled the organisation to respond to technology demands and risks which were then exacerbated because of the COVID-19 pandemic. The programme ran for over two years and it allowed most staff to immediately work from home with no business disruption, it also reduced many technology risks:

- Cyber Essential Plus accreditation was achieved, a UK government and National Cyber Security Centre certification scheme which demonstrates a minimum level of protection in cyber security.
- Computer operating systems for servers and laptops were updated.
- The majority of corporate data was moved to the Microsoft "cloud" (Azure / 365) for greater protection, resilience, accessibility and staff collaboration.

- A disaster recovery project improved the documentation and staff knowledge for the recovery of systems.

- A new secure network was implemented in the refurbished Wellington House.

- Cyber security awareness was improved via compulsory staff training.

- A cyber response plan was introduced so that the organisation is better able to react in the event of an incident. Cyber and data incidents have a single reporting process and these events are examined at the monthly Regulatory & Compliance Board.

- New virus protection software was installed on all corporate laptops with an updated ICT Security Policy and a revised Bring-Your-Own Device Policy.

2.2 Despite the above improvements, the risks of a cyber related incident are increasing, this is partly because the pandemic has caused a sharp rise in the number of cyber-attacks and cyber-criminals, it is a rated VERY HIGH RISK on the organisation's corporate risk register. In response to this and the need for further digital transformation, last autumn the Combined Authority commenced MCA Digital, a new two-year programme which includes projects that will address both cyber security risks and resilience risks, it contains:

- A Security and Information Management project to implement an information management strategy, roll out more staff training and improve technical security.

- A Cloud Infrastructure project to remove the remaining dependencies of Wellington House and to move virtually all systems and data into the Microsoft Cloud for greater protection.

- A Disaster Recovery project to formally implement a scheduled plan of simulated system recoveries.

- A SharePoint project to manage the migration of police and crime data into the Microsoft Cloud where it will be both highly secure and available for collaboration to approved individuals.

2.3 The Combined Authority has recently signed a contract with Microsoft for enhanced support, including for security. The organisation is also in the process of moving responsibility for managing key parts of the infrastructure to suppliers (firewalls and telephony), this is lowering cyber and resilience risks.

2.4 "CiSP" is a joint industry and government initiative (National Cyber Security Centre) set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, it includes the Combined Authority as a member. This is an invaluable source of information and advice for countering emerging risks, including those which are of an international nature. The Combined Authority is also a member of the Yorkshire & Humber WARP

(Warning, Advice and Reporting Point) where it benefits from security collaboration with regional public bodies including all the West Yorkshire District Councils.

2.5 Progress in implementing paragraphs 2.2 and 2.3 has been delayed because of higher-than-normal staff turnover for ICT engineering posts and longer than normal delays in associated recruitment. The organisation has approved a new Technical Security Lead position to oversee much of the required changes but this post has not yet attracted a satisfactory response and is currently being readvertised. In a highly competitive regional employment market for IT specialists, it is proving difficult to attract suitably experienced staff.

2.6 The Combined Authority has engaged with central government (Department for Levelling Up, Housing and Communities) over its cyber risk exposure. In February 2022 it received £175,000 of funding to implement an agreed Cyber Treatment Plan to make necessary improvements. It is expected that these implementation activities will be incorporated within the MCA Digital Programme.

2.7 Five years ago the Combined Authority experienced one major cyber incident when a member of staff inadvertently downloaded a personal email containing a “zero-day” virus (a brand-new virus which has yet to receive a fix from suppliers). Following this, personal email was blocked and many improvements have been introduced. There have been no other major cyber incidents.

2.8 In summary, the main cyber related risks for the Combined Authority are the following:

- The need to improve backup of data to provide greater resilience.
- The need to have systems to monitor IT audit files, malicious activities and provide alerts.
- The need to upskill both specialists in ICT Services and the wider staff for dealing with cyber threats.

2.9 Through agreed work which is in train the organisation will lower its cyber risks by implementing an agreed industry recognised information management strategy, upgrading its ICT infrastructure and having more robust operational processes. It should also be noted that:

- IT risks are carefully managed, including risks from suppliers and third parties.
- The Combined Authority’s incident response plans have recently been updated with greater clarity on the roles of staff.
- A Change Advisory Board in ICT Services meets weekly to implement agreed improvements.
- The organisation receives early warning information from the National Cyber Security Centre.

3. Tackling the Climate Emergency Implications

3.1 There are no climate emergency implications directly arising from this report.

4. Inclusive Growth Implications

4.1 There are no inclusive growth implications directly arising from this report.

5. Equality and Diversity Implications

5.1 There are no equality and diversity implications directly arising from this report.

6. Financial Implications

6.1 Approval has been given for £2.3 million through the Assurance Framework for MCA Digital of which over £250,000 will deliver security and resilience benefits. In addition, the Combined Authority has received £175,000 from central government to implement a cyber treatment plan.

7. Legal Implications

7.1 There are no legal implications directly arising from this report.

8. Staffing Implications

8.1 A project team is managing improvements to the organisation's cyber and risk posture via the MCA Digital programme. Current vacancies for Technical Security Lead and ICT Infrastructure Engineer require filling in order to accelerate delivery.

9. External Consultees

9.1 No external consultations have been undertaken.

10. Recommendations

10.1 That the Committee notes the report and provides any comments or feedback.

11. Background Documents

None.

12. Appendices

None.