West Yorkshire Combined Authority | Tracy Brabin Mayor of West Yorkshire

Report to:	Corporate Scrutiny Committee
Date:	1 March 2024
Subject:	**Cyber Security**
Director:	Alan Reiss, Chief Operating Officer
Author:	Ian Towner, Cyber Security Manager

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 detailing the relevant elements of the MCA Digital Programme.

1.2 Further analysis is provided in the exempt **Appendix 1.**

2. Information

Current Threats

1.3 The Cyber Security threats faced by the West Yorkshire Combined Authority are significant and the risk is rated as VERY HIGH on the organisation's corporate risk register. This is due to the significant number of attacks that are occurring daily against organisations in general, as well as the Combined Authority's association with the United Kingdom Government and the current geopolitical climate.

MCA Digital Programme

1.4 The MCA Digital Programme, which commenced in Autumn 2021, built on the previous Corporate Technology Programme (CTP) and includes some outstanding elements which were not completed as well as several projects that address both cyber security and resilience risks.

1.5 The MCA Digital project has several projects that are still in in progress, and these will further improve the overall security of the organisation. The ongoing projects are:

1.6 **Security Operations Centre** - ICT Services have procured a managed Security Operations Centre (SOC) service provided by Scottish managed services organisation BrightSolid. This service will provide 24/7/365 security monitoring of all the organisations systems, looking for suspicious or anomalous activity which could indicate a threat, investigating and neutralising these quickly. Most cyber-

attacks occur outside of business hours so this service will provide a very important detection capability. Work has started to onboard the organisation's systems and allow BrightSolid to tune their detection alerts, it is expected that the basic service will go live in April 2024, with the full implication to follow soon after.

1.7 **Disaster Recovery** - A procurement has recently started to obtain a partner to work with the organisation to deliver further disaster recovery solutions which covers all critical services and ensures a documented and tested recovery plan is in place should a major incident occur that requires it. It is expected that this work will be completed by the end Q2 2024.

1.8 **Software Allowlisting** - As part of the Cyber Treatment Plan, it was recommended that the Combined Authority should implement a software allowlisting solution to only permit trusted software to run on the organisation's laptops. This is a strong defence against cyber-attacks as it prevents malware and other malicious software from running. This work is expected to start Q1 2024.

1.9 **Patching and Vulnerability Management** - A procurement has been started to obtain a partner to provide additional skills and resources to ICT Services to enable the remediation of vulnerabilities and the automation of system patching. The objective is to put in place a sustainable patching and vulnerability management foundation and processes to ensure vulnerabilities are manageable and remediated within the timeframes required by the Government's Cyber Essentials programme. It anticipated that this work will be completed by the end Q1 2024.

1.10 **Cyber Essentials Plus (CE+)** - Cyber Essential Plus accreditation is a UK Government and National Cyber Security Centre (NCSC) certification scheme which demonstrates a minimum level of protection in cyber security. The Combined Authority previously held the accreditation however due to resourcing issues this accreditation lapsed. To obtain the accreditation the organisation must have in place patching and vulnerability management processes that meet the strict requirements set by the Cyber Essentials scheme. This requirement will be achieved through the procurement of a partner as detailed in 2.10. It is anticipated that the organisation will be in a suitable position to obtain Cyber Essentials Plus accreditation by the end Q2 2024.

Further analysis is provided in the exempt Appendix 1

<u>Cyber Security Workstreams</u>

1.11 Other risks identified and managed as part of business as usual (BAU) processes include:

1.12 **Bring Your Own Device (BYOD) solution** - The solution in place allows all staff to use their own devices to access corporate resources (SharePoint, email,

OneDrive etc). This presents a risk to both data leakage/loss and an increased risk of staff credentials being compromised due to using devices not managed and secured by the Combined Authority. A technical review is in progress to assess options to better secure both data and credentials when using BYOD as well as the assessment of risks associated with the use of BYOD which will inform proposed policy changes.

1.13 **Privileged Access Management** - The Cyber Treatment Plan, penetration testing reports and other audits have highlighted issues with ICT Services administration accounts having excessive permissions.

1.14 **Password Management** - The Combined Authority has embraced Windows Hello for Business (WHfB) which provides a very secure way to sign into the organisation's laptops, however passwords are still required and the strength of these has been questioned through penetration testing. The ICT Password Policy is in the process of being amended to improve the strength of passwords through the increase in length and using software to detect and prevent staff choosing weaker passwords.

Artificial Intelligence (AI)

1.15 The development of publicly available AI systems such as ChatGPT has generated a lot of interest and concern about how these systems could transform information management and society in general. The use of AI will clearly bring opportunities to organisations, but they also present threats, and due to the fast pace of change it is difficult to predict the true impact of either.

1.16 In the short-term AI will mainly affect the security of organisation by allowing attackers the ability to generate more convincing phishing emails and websites, building on an already successful method for obtaining credentials and propagating malware. AI will lower the barrier for novice cyber criminals and will make social engineering and reconnaissance easier. Sophisticated use of AI will, in the short-term, remain the preserve of nation state actors who have the funding and training to develop more advanced threats.

1.17 While cyber criminals will embrace AI, the same technology is being used to develop software that will make detection and prevention of cyber-attacks more automated and therefore more responsive to the increasing threat. Microsoft is leading the development of AI powered solutions with their Co-Pilot branded services such as Security Co-pilot. As the Combined Authority has deployed the full stack of Microsoft security solutions and the BrightSolid Security Operations Centre (SOC) also utilises Microsoft security toolsets, we are in a good position to benefit from advances in this area.

1.18 The business benefits of AI are already being seen with the implementation of Co-pilot in the Microsoft Edge browser, allowing anyone to use AI to generate text and

images as well as providing computer code samples which can be useful to IT workers. There is no doubt that this evolution provides exciting possibilities but there are risks, AI is not infallible and can provide inaccurate information. As an example, code generation by AI can be useful to help a less experienced developer to find a solution to a problem, however the code must be verified and understood to ensure it does what is expected, and it would be dangerous to rely on AI at this stage to generate code or text without errors or omissions.

1.19 ICT Services is investigating ways in which to leverage the advances in AI to help the organisation deliver services in the most efficient way possible. AI is a powerful technology that needs to be better understood before it can be deployed. With the AI building blocks of Cloud computing and its new data platform in place, the Combined Authority is in a strong position to develop AI goals, understand its potential impact on staff roles, establish how it could be used to aid organisation decision making and define how AI opportunities can be harnessed in an ethical manner.

1.20 An external consultancy will be engaged towards the end of 2024 to help define a three-year ICT strategy, including the following AI specific recommendations:

- AI principles, criteria for when the technology should be used.
- Lessons to be learned from what similar organisations are doing in this area.
- The Combined Authority service areas that would benefit the most from AI and what form implementation should take.
- AI governance and management of risks.
- An AI implementation roadmap.
- Whether there is the potential for advising regional businesses in this area and if yes how this could be approached.

Summary

1.21 In summary, the threats to the organisation are at an all-time high and these threats are not likely to reduce. Although a lot of work has been undertaken to improve the security posture of the organisation, there remain significant weaknesses and vulnerabilities which must be remediated, as a priority, to minimise the risk of a successful Cyber-attack. This work has the focus of a dedicated Cyber Security Manager who is responsible for ensuring the work is prioritised and the correct action is taken.

Further analysis is provided in the exempt Appendix 1

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 There are no financial implications directly arising from this report.

7. Legal Implications

7.1 The information contained in **Appendix 1** is exempt under **paragraph 3 of Part 1 to Schedule 12A of the Local Government Act 1972** as it contains information relating to the financial or business affairs of any particular person including the Combined Authority. It is considered that the public interest in maintaining the content of **Appendix 1** as exempt outweighs the public interest in disclosing the information, as publication could prejudice the financial or business affairs of the Authority.

8. Staffing Implications

8.1 There are no staffing implications directly arising from this report.

9. External Consultees

9.1 No external consultations have been undertaken.

10. Recommendations

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

11. Background Documents

There are no background documents referenced in this report.

12. Appendices

Appendix 1 – Cyber Security EXEMPT