CORPORATE AND REGENERATION SCRUTINY COMMITTEE – 9TH JANUARY 2024

SUBJECT: **CYBER/INFORMATION SECURITY UPDATE**

REPORT BY: **CORPORATE DIRECTOR OF EDUCATION AND CORPORATE SERVICES**

1. PURPOSE OF REPORT

1.1 The purpose of this report is to provide members of the Corporate and Regeneration Scrutiny Committee with a status update in relation to the Council's approach to Cyber/Information Security.

1.2 This update is aligned to the Council's Cyber Security Strategy ('Strategy') and Associated Action Plan, which were formally endorsed by Cabinet on 30 November 2022 and implemented in December 2022.

2. SUMMARY

2.1 Since implementation of the Strategy positive progress has been made in all of the critical success factors within the Strategy and Action Plan. It is important to acknowledge that the Council can never be 100% secure and there is further work to progress, however we are in a much stronger position than in December 2022.

2.2 Highlights the continuation of the positive work undertaken within both the Corporate and Education Cyber Security Forums, which are held regularly on a variety of Cyber Security issues. A positive example of the impact of the Education group, can be seen in Section 5.9 of this report. Within the Corporate domain, positive examples can be seen in the progress detailed within Section 5.10 of this report.

2.3 Introduction of a new Matobo 'Cyber Ninja' Training for all staff, with the ability to audit and track those who have completed the training. Circa 97% (as of mid-October 2023) of all corporate staff having completed the course.

2.4 To further illustrate our progress, the Council has the ability to track our Microsoft Secure Score, which is a KPI generated on the Microsoft platform on how secure our Microsoft 365 environment is. In July 2023, our score was circa 65% and as of October 2023 it is in excess of 80% with further improvements expected over the coming months. For context, the average score for similar organisations is 47%.

3. RECOMMENDATIONS

3.1 To note the status update and the progress made in relation to Cyber/Information Security since the implementation of the Council's Cyber Security Strategy and Associated Action Plan in December 2022.

4. REASONS FOR THE RECOMMENDATIONS

4.1 To ensure that the Council is continuously monitoring and improving its Governance and Cyber/Information Security arrangements.

5. THE REPORT

5.1 ACCREDITATION

5.1.1 Positive progress in achieving PSN compliance has been made, on our most recent submission the Council were deemed 'In Remediation' and since that point, there has been continued communication with our assessor regarding our application. It is hoped that PSN accreditation will be secured ahead of the results of our upcoming Information Technology Health Check ('ITHC'). The outcome of the ITHC is due in January 2024.

5.1.2 If it is not possible to secure the accreditation in the coming months, the Council will be in a good position to achieve PSN compliance moving into 2024 due to the positive relationship we have now developed with our assessor, leading to a more complete understanding of the requirements and mitigations expected.

5.1.3 Due to the conversations undertaken with our assessor, approval is now being sought from JARD to enable our staff in Trading Standards to access a particular platform, which is used to manage Confiscation Orders. This is currently one of the biggest issues caused by the Council not being PSN compliant and again are hopeful to resolve imminently, regardless of our PSN status.

5.1.4 Participation in a phase 1 pilot of the Cyber Assessment Framework ('CAF') in early 2023, this exercise introduced us to the CAF process and a different method of evaluating our organisation. Since then, we have closely followed both the Welsh and English pilot schemes and the lessons learnt for further developments.

5.1.5 Whilst we await next steps from Welsh Government in relation to CAF, the Council has been able to align more closely to the requirements through the work completed to date, together with the projects we have planned moving forward. It is anticipated that we will revisit and measure ourselves against the CAF in early 2024 to highlight our progress, together with identifying additional areas to strengthen our approach to Cyber/Information Security.

5.2 PERFORMANCE INDICATORS

5.2.1 One of our most prominent key performance indicators ('KPIs') used to measure our overall progress has been our Microsoft Secure Score. Also, another key metric being the completion information in relation to the Matobo Cyber Ninjas Training.

5.2.2 Our Microsoft Secure Score is a Microsoft generated KPI of how 'secure' the Council is from the viewpoint of our Microsoft Defender suite. This includes scoring on how well configured our different Defender aspects are, together with the rules that are established on our system. Previously our score was consistently in the range of 60-65%. However, due to the ongoing work in this area, we have seen this increase to in excess of 80%. For context, an average Council estate scores in the range of 45-50%.

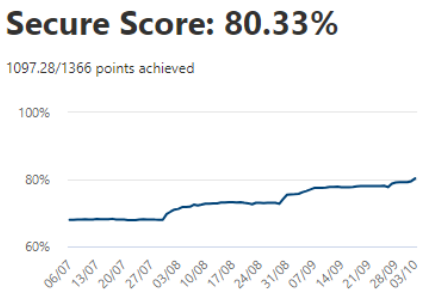

Figure 1- Microsoft Secure Score

5.2.3 Additionally, due to the audit capabilities of the Matobo 'Cyber Ninja' Training, there is the ability to track the percentage of all staff that have completed the training, which hadn't been possible previously. The progress made in this area, both in terms of numbers and evidence will go a long way to ensuring the Council can positively answer these criteria in the various audits that are used to measure our organisational cyber posture.

5.3 TRAINING

5.3.1 The Matobo 'Cyber Ninja' Training has been a big success. As of mid-October 2023, 2785 members of staff have completed the training, which equates to circa 97% of those staff members with a corporate email account. Furthermore, a significant amount of positive feedback about the approach and presentation of the training has been received.

5.3.2 Similarly, 10 Councillors have completed their version of the Matobo 'Cyber Ninja' Training and 3 are currently in progress. With positive feedback being received from those who have so far completed the training. Help and assistance have and will continue to be offered to Councillors with the opportunity to meet and complete the training with one of the Security Team to help explain and talk through some of the queries that may arise throughout the course.

5.3.3 Work is continuing in relation to our Incident Response Policy and Procedure, with the aim of conducting exercises for key members of staff to run through the process. This will allow those involved the chance to see how the procedure works 'in practice', as well as providing the chance for the procedure to be tested and to highlight any blind spots or areas that need further clarification.

5.4 CULTURE

5.4.1 The Cyber Security culture within the organisation is growing, and despite sometimes being seen as a blocker, we are in a good position due to a combination of awareness raising, training and various pieces of work to implement controls on certain key areas, such as the implementation of Azure AD Password Protection for all corporate staff.

5.4.2 Currently carrying out an awareness campaign for Cyber Security Awareness Month, which has involved us providing communications to all staff via email and the intranet across a variety of subjects, such as QR code phishing and ransomware, throughout the month of October. Numerous communications have also been issued throughout the year, especially if there has been a rise in a particular type of phishing email as an example.

5.4.3 Security staff continue to participate in the Warning Advisory and Reporting Point (WARP) and Gwent Local Resilience Forum (LRF) meetings, which provides the

latest information on Welsh/Gwent Cyber projects. Most recently, the introduction and implementation of the Gwent LRF Cyber Incident Response Plan, which provides all participating organisations in the area with the required procedure should an incident occur which requires the notification of the wider group.

5.4.4 In addition to the above, the Council's Security Team remains vigilant to the changing landscape of Cyber Security and endeavour to recommend best practice processes and procedural changes that will allow the Council to strengthen our Cyber resilience not only for the next week but in excess of 3 years plus. Examples includes the evaluation of passwordless authentication, if and how the Council can use the various generative AI tools that are being introduced, such as the upcoming Microsoft copilot. Also ensuring the creation of adaptable policies, where it's possible, so that the Council is able to adjust with the landscape without having to continue to re-write policies.

5.5 SUPPLY CHAIN

5.5.1 A vitally important area that requires further development, however it is important to highlight that all public and private sector organisations understand the need to learn and improve ways of working. It is well publicised that more and more organisations are being compromised via their supply chain. Work has begun in conjunction with staff across Procurement and Information Services that will aim to ensure we understand and ask the right questions of our third parties at the outset and also ensure regular checks and due diligence is undertaken via proactive contract management. Ensuring that we maintain up to date and accurate information throughout the lifespan of applicable contracts.

5.5.2 As part of the above project, the initial phase is aimed at our critical digital services/ IT suppliers. This will allow us to evaluate a crucial aspect of our supply chain, thus adding to and strengthening our Security posture and building upon the work that has already been done in this area, such as the development of our Cloud Compliance Assessment for all cloud services, which is based on the NCSC's Cloud Security Principles.

5.6 INCIDENT REPORTING

5.6.1 The Gwent LRF Incident Response Plan has now been published and is live. The document provides the Council with a step-by-step guide should an incident occur, that is of sufficient size and impact that we would need to alert other local organisations. Whilst this is a process that would be expected of us as a member of the Gwent LRF forum, there is now a clear procedure to follow, together with other important and relevant information.

5.6.2 This information has proven useful and beneficial when updating our own Incident Response Plan, which is currently underway. The Gwent LRF Plan will be used and where applicable incorporated within the Council's specific Plan thus ensuring a consistent approach that escalates appropriately depending on the severity and impact of an incident. The Plan also includes incident-specific playbooks. These are adjusted actions to be taken for specific scenarios. For example, but not limited to, if the Council is hit by a Phishing attack the response will be different than being hit by a Ransomware attack.

5.6.3 In addition to the above policies and procedures, an exercise program is currently being considered that will enable the Council to undertake a run through of our policies and procedures. It is anticipated that this will be undertaken on an annual basis together with multiple table-top exercises to hopefully ensure that our plans, processes and procedures remain relevant and accurate, so if an incident were to happen then

our response is fit-for-purpose.

5.7 DOCUMENT REVIEW

5.7.1 As stated in Section 5.6 immediately above, work is well underway on reviewing and updating our Cyber Incident Response Policy and Plan.

5.7.2 To support our approach with the Supply Chain, updates have been incorporated within the Council's Data Processing Agreement. Together with the inclusion of additional Cyber/Information questions within the Council's e-tendering system, Proactis. In time this will allow the Council to search and filter on economic operators within our Supply Chain that have accreditation to a Cyber Security standards together with the associated evidence. In addition, this will allow us to identify economic operators that require further development in this vitally important area, thus allowing the Council to implement risk mitigation measures if and when necessary.

5.7.3 In the immediate, future work will be commencing on updating our Cyber/Information Security Policy. The revision will incorporate and reflect our current working practices, bringing together a number of our recent policy/procedural changes, such as formalising our approach on Bring Your Own Device (BYOD), including mention of the Conditional Access Policy as well as our Cyber Incident Response Policy and Playbooks.

5.8 SECURITY OPERATIONS CENTRE ('SOC') / SECURITY INFORMATION AND EVENT MANAGEMENT ('SIEM') PROJECT

5.8.1 The Welsh Government are looking to introduce a cross-council Security Operations Centre ('SOC') solution. This will involve the Council 'plugging into' the SOC and provide information already created and available, in the form of logs, so they can monitor and highlight any possible malicious patterns and activities.

5.8.2 There has been delays with the Welsh Government procurement procedure, which is currently planned to commence and go live at the end of October 2023, it is currently hoped the implementation will commence in early 2024. There remains uncertainty regarding the extent of the project and potential solutions as undoubtedly there will be differences between bidding organisations. However, once the procurement procedure commences further information will be available to understand matters in more detail.

5.8.3 Due to the prevalence of E3 and E5 Microsoft licensing across Welsh Councils, it is highly likely the solution will be compatible with Microsoft. Therefore, to ensure the Council can take advantage of any potential solution work has been undertaken and will continue on better utilising and configuring our Microsoft Defender suite, in line with Microsoft recommendations. This will undoubtedly benefit the Council on whether the SOC project is implemented or not, subject to the outcome of the procurement procedure.

5.8.4 Furthermore the Council is due to undertake a Microsoft funded Proof of Concept ('PoC') with a third party, namely Bridewell. This PoC will further enhance our knowledge and understanding of how the current information within Microsoft Defender can be used within Microsoft Sentinel. This will also be beneficial in terms of understanding potential costs and implementation if this platform is identified as the preferred option following conclusion of Welsh Government's Procurement procedure.

5.9 EDUCATION

5.9.1 The Education Cyber Security Forum ('ECSF') have continued on a monthly basis since the first meeting in May 2022. The ECSF includes staff from Schools Support, Information Security and Information Governance attending and working to improve the Cyber/Information Security within the learning domain. Undoubtedly the ECSF has been a catalyst for the improvements made across the Learning domain as an example the improvements made in software patching (amongst others).

5.9.2 Work is continuing on the outstanding vulnerabilities and issues with the aim of maintaining this level of Cyber/Information Security, however it is important to highlight the impact that has been achieved in the recent past.

5.9.3 Staff with ECSF have strengthened ties and working relationships with School representatives in a variety of ways. Examples include:

- Schools Cyber Incident Report Procedure was drafted and ratified by the ECSF and subsequently issued to all Schools for ratification via Governing bodies.
- ECSF issued a 'Newsletter' containing pertinent and succinct information relating to Cyber/Information Security and regular communications will continue with positive feedback received.
- In April 2023 an initial meeting was arranged with the Secondary Schools Network Managers to discuss a variety of issues. Additional meetings have and will continue as business as usual.
- In June 2023, access to Lansweeper was given to Secondary Schools Network Managers, to benefit from the technical data all the PCs and Servers within their individual Schools. The response has been very positive, the provision of direct access to reports for the Network Managers will undoubtedly assist the Council in our aims, but also demonstrates trust and collaborative working with our Schools.
- Members of the Security Team have joined the Jisc Cyber Security Community, made up of over 1000 professionals responsible for Cyber Security matters across the Education sector in the UK.
- Discussions being held with representatives of a third party, namely, NCC Group with the aim of conducting a gap analysis against the technical requirements of the Education Digital Standards, thus enabling the Security Team to further enhance our knowledge and prioritise our next phase of work across of Learning domain.
- Continue to build upon the positive work in relation to our Corporate approach to Password Security and look to implement a comparable standard (if not the same) within the Learning domain.

5.10 CORPORATE

5.10.1 Similarly, the Corporate Cyber Security Forum ('CCSF') has continued on a monthly basis. The CCSF includes staff from Information Security, Digital Solutions, Digital Infrastructure and Corporate Support attending and working to improve the Cyber/Information Security within the Corporate domain, in line with the Critical Success Factors within our Cyber Security Strategy. As with the ECSF, the CCSF has been a catalyst for the improvements made across the corporate domain, as an example the improvements made with regard to our corporate passwords (amongst others).

5.10.2 The Council introduced and implemented Azure AD Password Protection. This prevents users from setting passwords which don't meet our required complexity standard and allows certain passwords/words to be blacklisted. In essence all those passwords that were 'cracked' have been added to the blocked list and cannot be used.

5.10.3 As of mid-October 2023 and in preparation for the next ITHC a password cracking exercise was undertaken. The exercise included checking passwords against the last 5 years of 'cracked' passwords internally, together with against the most frequent 100,000 passwords globally. The upcoming ITHC may identify further password vulnerabilities as the organisation utilises more up to date and complex methods.

5.10.4 Staff within CCSF have strengthened ties and working relationships corporately in a variety of ways. Examples include:

- CCSF have worked to remediate the vulnerabilities found in the latest ITHC and ensure they are not present across the corporate domain, as well as in the 10% checked in the ITHC, with the majority of the remaining vulnerabilities being issues with our Supply Chain and work is ongoing to address these.

- Multiple project groups have been established with members of Information Security and Digital Services involved from the start to manage IT projects across the Council. One group has been involved with the ongoing work to move the critical applications to Software as a Service (SaaS) solutions to improve our resilience. Another such group was set up in preparation for the 2012 servers end of life (10 October 2023).

- There have been general positive communications through updates and informational messaging through the Communications Unit between the Security Team, the SIRO, the Director and the Council, such as the current communications around Cyber Security Awareness Month, as well as previous communications sent to all users on Password Day and when we see a noticeable uptick in certain phishing tactics.

- CCSF have worked on vulnerability reduction and increasing our security posture in general. Ensuring the latest NCSC guidance and 10 Steps to Cyber Security is being followed, such as ensuring the latest patches are installed where necessary, especially where the vulnerability is actively being exploited or poses an imminent risk. An example of where this approach has helped protect the Council is where Digital Infrastructure Manager Jonathan James was able to update our Citrix NetScaler on the 19 July 2023 and mass exploitation of the issue by cybercriminals began on the 20 July 2023.

- The CCSF, and the wider Security and Digital Services Team have begun shifting focus to Windows 10, which will be unsupported after 14 October 2025. This early focus will allow the upgrade away from Windows 10 to become BAU and mean as we close in on the 2025 deadline, any 'problem' systems would have been identified and have an approach and any mitigations agreed in a timely manner.

- The Security Team are in the process of implementing the use of Microsoft Attack Simulator. This will be used to send fake phishing emails to staff twice a year to determine areas needing further education/training and act as 'little and often' training in addition to our annual training resource, currently the Matobo 'Cyber Ninja' Training.

- The Council have signed up to a variety of NCSC approved schemes to provide additional monitoring, such as Police Cyber Alarm and NCSC Notifications. Additionally, the Security Team continue to participate in a variety of wider

forums, such as Warning, Advice and Reporting Point (WARP) and Gwent LRF and provide updates to the CCSF as necessary.

5.11 Conclusion

5.11.1 The Council is in a much stronger position than in December 2022 as progress has been made across all critical success factors within the Strategy and Action plan.

5.11.2 The Corporate and Education Cyber Security Forums continue to have a positive impact on the Council's Cyber Security posture and act as a key contributor for new and ongoing improvements.

5.11.3 The rollout of the new Matobo Cyber Security Training has been a success, with circa 97% (as of mid-October 2023) of all corporate staff having completed the training.

6. ASSUMPTIONS

6.1 There are no assumptions in respect of the current recommendations of this report.

7. SUMMARY OF THE INTEGRATED IMPACT ASSESSMENT

7.1 There is no Integrated Impact Assessment in respect of the current recommendations of this report.

8. FINANCIAL IMPLICATIONS

8.1 There are no financial implications in respect of the current recommendations of this report.

9. PERSONNEL IMPLICATIONS

9.1 There are no personnel implications in respect of the current recommendations of this report.

10. CONSULTATIONS

10.1 This report has been sent to the Consultees listed below and all comments received are reflected within this report.

11. STATUTORY POWER

11.1 NCSC 10 Steps to Cyber Security

Author: Matthew Cuthbert, Information Security Manager
(cuthbm@caerphilly.gov.uk)

Consultees: Cllr Nigel George, Cabinet Member for Corporate Services, Property and Highways,
Corporate Management Team (CMT) on 16 November 2023,
Richard (Ed) Edmunds, Corporate Director for Education and Corporate Services,
Elizabeth Lucas, Head of Customer and Digital Services,

Ian Evans, Procurement and Information Manager,
Customer and Digital Services Management Team,
Wesley Colyer, Senior Information Security Officer,
Edward Thomson, Information Security Officer,
Mackenzie Evans, IT and Digital Support Apprentice.
Cyber Security Forum, Corporate,
Cyber Security Forum, Education.