Agenda Item No: **XX**

CITY OF WOLVERHAMPTON COUNCIL

Audit and Risk Committee

25 July 2022

Report title	Cyber Security Statement June 2022	
Accountable director	Charlotte Johns, Director of Strategy	
Originating service	Digital and IT	
Accountable employee	Jaideep Ghai	Head of Digital and IT
	Tel	01902 552072
	Email	jai.ghai@wolverhampton.gov.uk
Report to be/has been considered by		

Recommendation for action or decision:

The Audit and Risk Committee is recommended to:

1. Review and comment upon the contents of the Council's Cyber Security Statement for June 2022.

1.0 Purpose

1.1 The purpose of this report is to provide an update regarding how the City of Wolverhampton Council (CWC) are managing evolving Cyber threats, the measures in place and work in progress to ensure on-going protection

2.0 Background

2.1 The Cyber threat landscape is continuously evolving with new vulnerabilities being published weekly and with the on-going conflict in the Ukraine, the Cyber threat Level has been increased to HIGH by the National Cyber Security Centre (NCSC). The NCSC have emphasised the need to be vigilant and to ensure robust processes exist to minimise and prevent any compromise.

2.2 CWC have actively been working on NCSC advice to ensure our data, workforce and technical architecture are continuously protected as well has acting on emerging threats and counteracting them as soon as they are identified. Alongside this, key findings from the NCSC Annual Active Cyber Defence Programme Report (ACD) have been reviewed to ensure compliancy and that threat mitigation measures are actively deployed.

2.3 CWC are always working with trusted partners to ensure Cyber defences are robust, in line with best practice and any vulnerabilities identified are plugged before they are exploited.

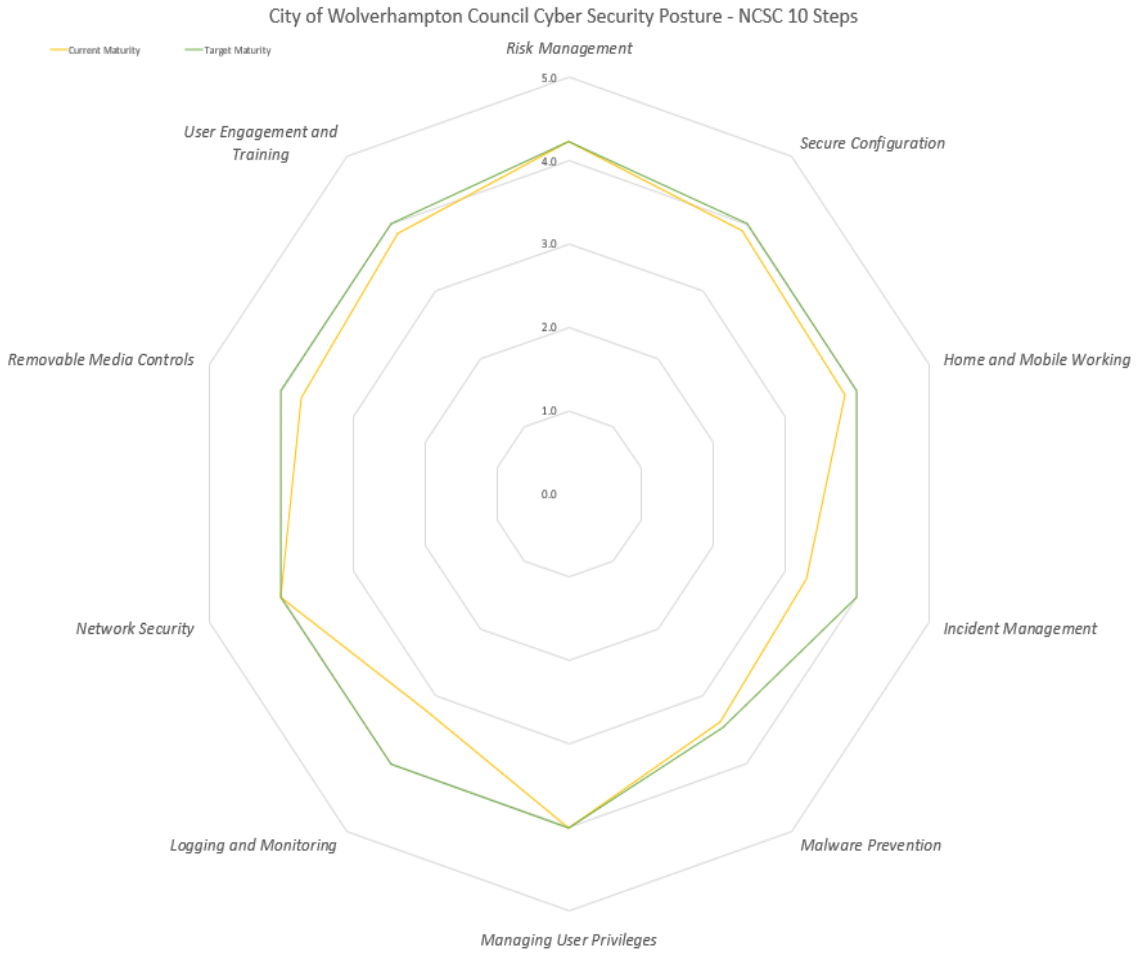
3.0 Progress, options, discussion

3.1 Cyber Security is a key priority for the Council and monitored rigorously via the strategic risk register. CWC is one of the few councils in the country that are Public Services Network (**PSN), Cyber Essential Plus certified**, Payment Card Industry Data Security Standard (**PCI DSS)** and NHS Information Governance (**NHS IG) Toolkit** accredited. Continued accreditation involves auditing and testing of Digital and IT systems and controls by a 3rd party throughout the year.
In March 2022, CWC PSN accreditation was recertified and currently working towards Cyber Essential Plus recertification which expires in September 2022. The recertification process involves engaging with a 3rd party who have undertaken active network scans to identify vulnerabilities which have been remediated. These 3rd party reports are submitted to central Government as evidence that CWC meets and exceeds stringent controls required for transactions with Government bodies

3.2 CWC have undergone Internal and External audits over the last few months to assess its Cyber and Disaster Recovery capabilities, and both identified **no serious issues** and recommendations made have been programmed to be completed by September 2022. Digital and IT have also used this opportunity to revise its Cyber Incident response plan, in partnership with our colleagues in Information Governance and Resilience, to meet the challenges of the Cyber Security landscape.

The Local Government Association (LGA) Funded Audit – As reported in the last briefing note CWC were awarded monies to engage with an external Cyber security expert to benchmark CWC again NCSC Cyber Security best practices. The outcome of the engagement was as below:

""The City of Wolverhampton Council has a strong cyber security posture and our recommendations are mostly minor controls to consider concerning Incident Management, Logging and Monitoring and Removable Media Controls. In a lot of these cases you are already considering tooling or have exercises planned in the not-too-distant future"



3.3 Digital and IT in partnership with the Resilience team undertook several events during Business Continuity week commencing 16th of May 2022. These included:

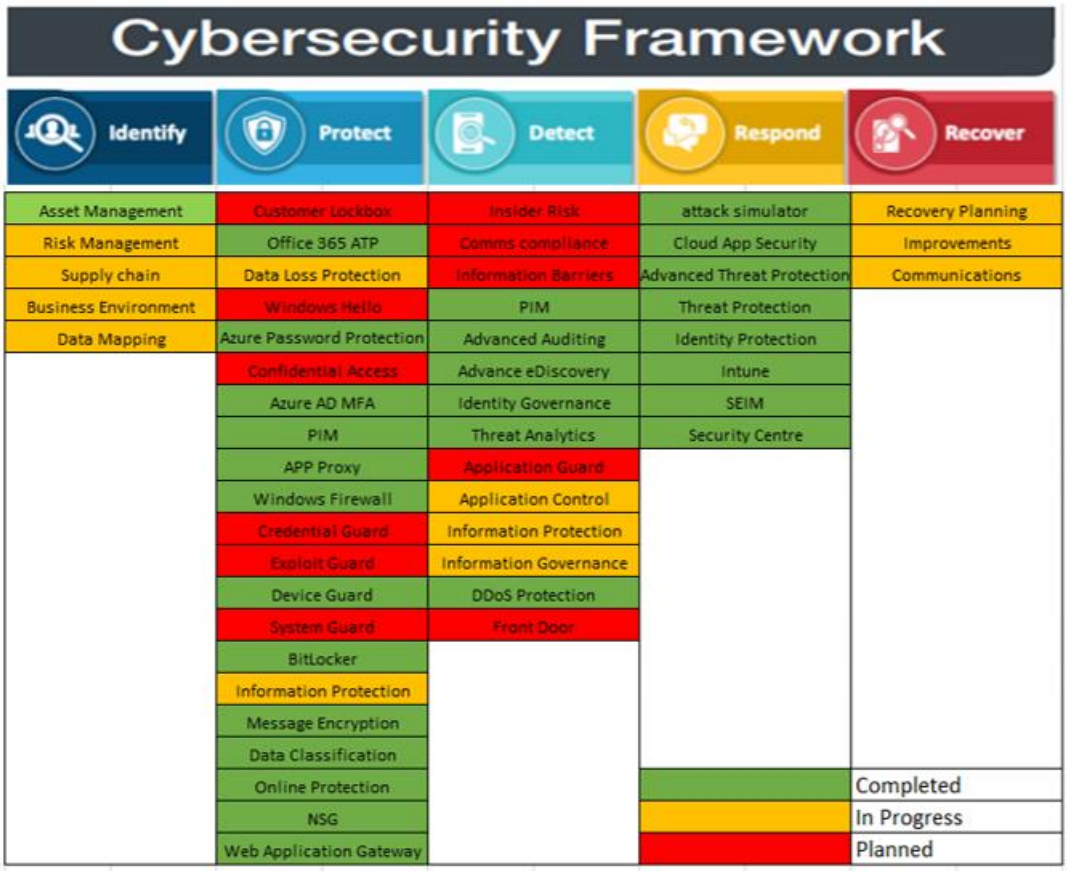
- Phishing exercise with the Multi Agency Safeguarding Hub (MASH)
- NCSC Ransomware out of the box exercise
- City People articles throughout the week to re-affirm the need to be vigilant in the hybrid world

Digital and IT worked collaboratively with the Resilience Team to simulate potential attacks and it enabled Digital and IT's Security Team assess the quality of the CWC incident

response plan and amend it accordingly. Further such events will be scheduled for later this year, including an exercise with SEB.

To complement the events, Digital and IT procured specialist Cyber training which the Business Critical team will be engaging SEB and Councillors over the coming months.

3.4 To reduce the impact of cyber-attacks, in particular ransomware, and to maintain our strong security position, Digital and IT continue to deliver against the following key actions, which are resourced in the capital programme.



Key deliverables in the coming months are:

- Reducing the Cyber Attack surface area by introducing endpoint controls that manage known attack vectors like unapproved USB devices
- Backup Immutability to allow failsafe recovery after ransomware attack
- Enhance Employee Cyber aware training
- Automated response system for Cyber incidents using security toolset
- Risk assessment for Supply chain attacks
- Removal of unsupported applications from Network
- Continued partner working with Information Governance and Resilience Teams
- Migration of Shared Data to Microsoft Cloud for continued protection

3.5 LGA funding has been awarded to the CWC to Digital and IT to train our staff to security specialist to Certified Information Systems Security Professional (CISSP) standard. CISSP is a highly sought-after certification which is focussed on Security Threat Management and staying on top of security trends. Having a CISSP working for CWC will help to ensure best security practises are maintained and robust and stringent measures are in place to counter threats

3.6 To counter emerging cyber threats requires flexible and agile policies along with support from the Senior Executive Board to allow for a rapid response. Several initiatives are being worked on that will be presented to SEB for support:

- Bring your own device (BYOD) – Working with information Governance, policies are being developed to allow for the use of personal devices to access corporate data within a secured container on the device. Microsoft Intune allows for app protection policies which enable the use of corporate data securely using Company Portal which allows the transition from a fully managed devices to unmanaged with protection.
- Unified Labels protection policies – CWC have deployed labelling policies that ensure data is classified at the time it is saved or sent to other people. To ensure that our data is used only by the intended recipients and not shared, protection policies are being worked which enable Council employees to manage how the data they have shared is used. This will allow employees to revoke access or be as granular as to restrict the likes of being able to print or forward the data.
- To maintain our Security certifications requires that all endpoints run vendor supported versions of software which requires continued investment on hardware. At times this may necessitate the replacement of the device for continued access to the Council's network.

4.0 Financial implications

4.1 There are no financial implications arising from the recommendation in this report. [AS/150722/R]

5.0 Legal implications

5.1 There are no legal implications arising from the recommendation in this report beyond those set out clearly in the Annual Governance Statement and the strategic risk register report. [DP/150722/C]

6.0 Equalities implications

6.1 The Council's governance framework underpins the Council Plan, which itself is guided by consultation and equality analysis, and thereby aides the Council in its ability to meet its equality objectives

7.0 All other implications

7.1 There are no other implications arising from the recommendation in this report.

8.0 Schedule of background papers

8.1 None.