



Digital & IT Cyber Security Update

June 2022

Jaideep Ghai

Background

- Cyber threat landscape is continuously evolving, highlighted by the weekly publication of new vulnerabilities and the conflict in the Ukraine.
- This is reflected by the Cyber threat level being increased to **HIGH** by the National Cyber Security Centre (NCSC)
- Emphasis placed on robust processes to minimise and prevent any compromise by the NCSC and be extra vigilant.
- Digital and IT take any threat seriously and protecting our network is of utmost importance and priority.

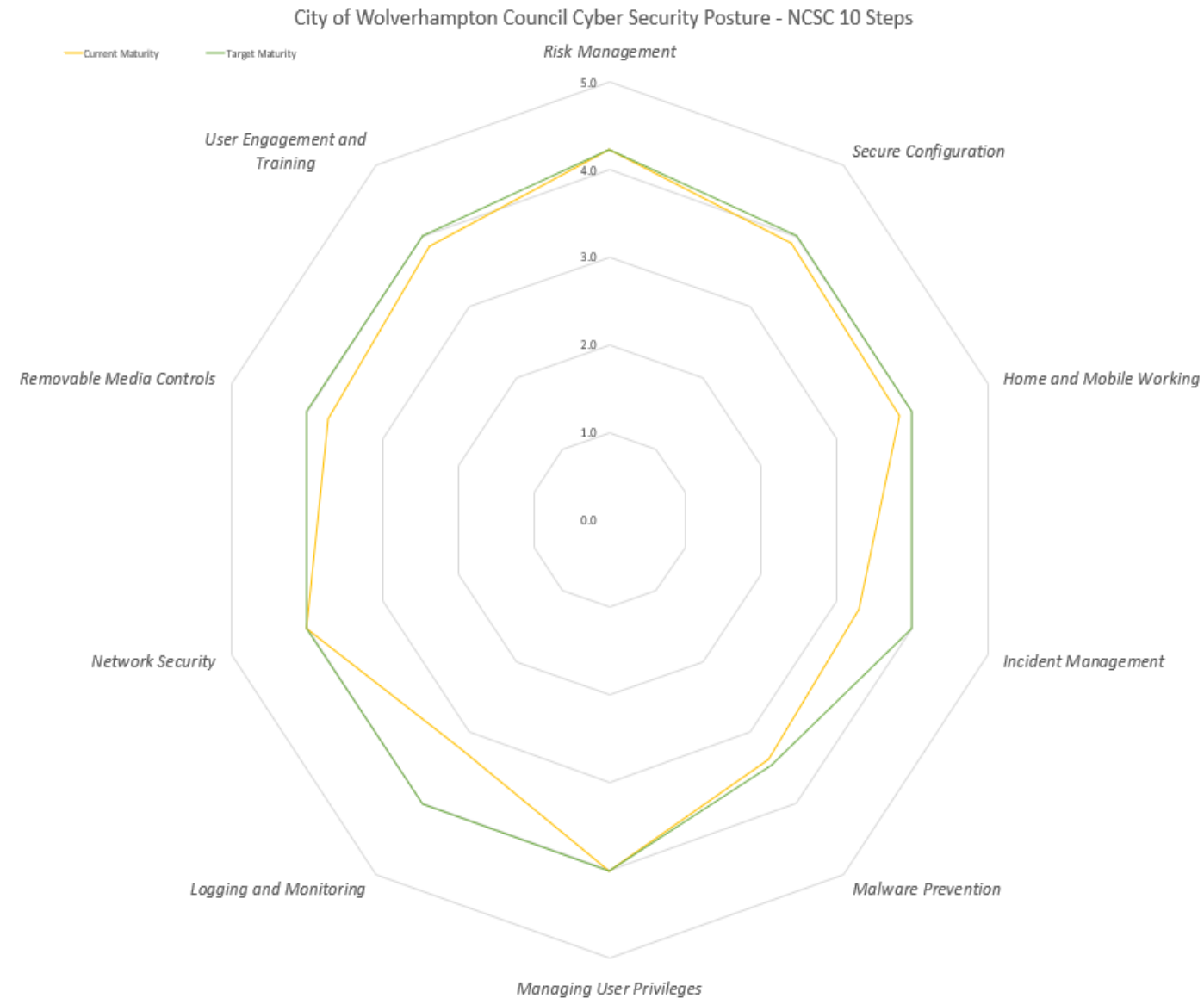


Stats provided by Government IT Security Conference

Deliverables and Work Undertaken by Digital and IT to Minimise Threats

- Benchmarking exercise completed comparing CWC against NCSC Cyber Security best practices with external Cyber Security and the outcome from the Local Government Association (LGA):

‘The City of Wolverhampton Council has a strong cyber security posture, and our recommendations are mostly minor’
 - Incident Management, Logging and Monitoring, and Removable Media Controls.
 - We are already considering tooling and have exercises planned in to resolve these issues.
- LGA funding awarded to CWC to train Digital and IT staff to Certified Information Systems Security Professional Standard



Deliverables and Work Undertaken by Digital and IT to Minimise Threats

- Continuously reviewing and implementing NCSC advice
- Deploying threat mitigation measures
- Working with trusted Partners to maintain and further strengthen our robust Cyber defenses
 - 3rd Parties actively scanning our network to identify vulnerabilities which have been remediated
 - These reports submitted to Central Government as tangible evidence CWC exceeds stringent controls required to transact with Government bodies
- Cyber and Disaster Recovery Capabilities assessed via internal and external audits
- Adopting Best Practice by plugging any vulnerabilities identified immediately
- Primary Security Network Accreditation recertified
- In partnership with the Resilience Team, Digital and IT undertook a few events during Business Continuity Week



Planned Activities/Next Steps

- Implementing recommendations Local Government Association
- Train Digital and IT staff to Certified Information Systems Security Professional Standard via LGA funding
- Recommendations from internal and external audit of Cyber and Disaster Recovery Capabilities to be implemented
- Automated response system for Cyber Security Incidents
- Backup Immutability enabling failsafe recovery following ransomware attack
- Introduction of USB and Application controls
- Enhance Employee Cyber Security Awareness training
- Removal of unsupported applications from the Network
- Migration of Shared Data to Microsoft Cloud
- Continued collaborative working with Information Governance and Resilience Teams
- Retain existing Cyber Security Accreditation i.e., Cyber Essential Plus



Digital&IT

[Thank you / Questions text]