CITY OF WOLVERHAMPTON COUNCIL

Appendix 3

Update on Selected Risk for Review

Risk title and description	Previous score (Feb 2019)	Direction of travel	Current score (May 2019)	Target score and date
Cyber Security Failure to maintain a high level of cyber security (technology, processes and awareness) throughout the Council may result in cyber-attacks and theft or loss of confidential data leading to financial penalties, reputational damage and a loss in public confidence. Risk owner: Gail Rider Cabinet Member: Cllr Sandra Samuels	12 **Amber**		12 **Amber**	10 **Amber** Ongoing – Dependent on cyber world-wide cyber incidents

1. Background

1.1 At the March 2019 meeting of the Audit and Risk Committee, members requested further information and assurances in respect of strategic risk 23 – cyber security be provided to the Committee by the risk owner. This report updates the Committee on the progress made by the Council in this area and the further actions required to manage the risk. The Council's Head of ICT will also attend the meeting to address any further assurances that the Committee may require.

1.2 The Cyber Security risk was first identified for inclusion in the strategic risk register by SEB in January 2016. At this time, the risk was assessed as 15 (red).

1.3 A Cyber-attack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually, the attacker seeks some type of benefit from disrupting the victim's network, often related to theft of data. Cyber security relates to security measures put in place to protect information (data) which is held digitally. It is imperative that the systems and data owned by the Council are fully protected against Cyber-attacks.

1.4 ICT play a key part in the delivery of robust security protocols, protecting network, applications and the authority's data. Working in partnership with the internal Information Governance (IG) team, a vigorous set of procedures, form an integral part of ICT's security role within the organisation. It must be noted that every member of staff within

the authority, has a personal responsibility in keeping the council safe from attacks. This can only be achieved by staff following all policies and procedures thoroughly, therefore reducing the risk of Cyber-attacks and any subsequent impact on critical services.

1.5 A decision was made in 2016 as part of the ICT strategy to adopt a "Cloud First" approach for the storing of council data, including the management and hosting of applications. This decision was made in line with a thorough review of options available. Although much of the Councils data is stored in the cloud, the authority also has an onsite data centre which houses a range of servers which manage a variety of applications, these are either not suitable to be migrated to the cloud or suppliers and their applications are not yet ready to work in this way. Where data is stored on servers on site, this is referred to as "on prem" data storage. The Council has a secondary data centre at Stafford, where a replication of the data centre at the Civic is housed. This forms part of the Disaster Recovery (DR) strategy, where Stafford would be used to replicate services should the authority have an incident at Civic where access to on prem data was not available.

1.6 Where information is required to be shared, ICT ensure that all present and future procurements conform to ISO 27002, the international standard for Information Security Management. (ISM) https://en.wikipedia.org/wiki/ISO/IEC_27002

2.0 Risk mitigation

2.1 There are key objectives to be considered when managing Cyber threats and incidents. ICT in partnership with IG ensure these are consistently complied with. The bullet points below set out the objectives. ICT work consistently to deliver against each of these:

- Defend – Defence against Cyber threats.
- Deter – The detection, understanding, investigation and disruption of hostile Cyber actions, which could lead to prosecution.
- Develop – Innovate, research and develop Cyber internal expertise that will meet and overcome future threats.
- Review – Consistently review Cyber security updates and guidance form the Governments, National Cyber Security Centre (NCSC).
- Profile – As members of the Public Services Network (PSN) Councils are required to develop their own threat profiles to ensure continued compliance.

2.2 ICT take a preventative approach ensuring all measures are taken to protect information from unauthorised modification, destruction or disclosure whether accidental or intentional. These measures include a combination of legacy and next generation security, combined with user awareness training and focused training for ICT staff.

2.3 ICT Policies consist of several operational security documents which are split between user type policies such as password procedures and internal operational policies such as authentication and patch procedures. The objective of these policies is to ensure the highest standards and best practice are in place, ensuring information security is maintained across the council. New password standards have caused some concerns with staff, due to the complexity. ICT take security seriously and understand the impact of a major incident, therefore the setting of password standards has been set at a complex level to reduce likelihood of attack, these are also in line with standards

recommended from Microsoft. (MS). The major threat to any business's data is generally that of individuals. Internal staff are possibly unwittingly one of the highest threats to security, particularly when policies are not followed. Hackers are by far the greatest threat, these are managed by encryption, firewalls, anti-virus products and patching of software. No business can be 100% protected, new threats are consistently tried by external hackers, ICT keep ahead of the game by applying all the above procedures, following guidelines and keeping abreast of new information.

2.4 Next generation firewalls conduct deep inspections of the network traffic, as it navigates the network combined with a live database of known threats received from the internet. These are managed by ICT, any threat detected is instantly blocked.

2.5 Traditional anti-virus and device lockdown methodologies are used on the network and use the latest software, these are updated continually. These run in the background without causing any effect on service provision. ICT use multiple anti-virus engines from different vendors which provide a higher level of protection and bring a more rigorous approach to defence.

2.6 Staff awareness training is a programme of training which highlights data/security risks. This includes sharing an understanding of "phishing" campaigns and completing a mandatory training course which all employees must complete, this course focuses on data security. Phishing campaigns involve targeting a wide group of staff within the organisation by sending out an email that entices users to perform a task, such as providing log in credentials. We look to entice staff to open a malicious attachment or click on a bad link. The awareness previously conducted should equip staff with the knowledge of how to spot a suspicious email and not respond, this is an excellent way of testing staff knowledge.

Regular "phishing" campaigns are run in partnership with IG to ensure staff have a good understanding of the risks to the authority. Information from phishing campaigns to date demonstrates an excellent level of understanding across the authority. Where staff open an email in error, this is reported and the IG team work with managers to re-enforce training and highlight the risks to the authority.

2.7 Cloud storage is not new, the technology continues to evolve, offering secure levels of data storage and an opportunity to secure effective DR procedures with ease. The authority takes a pragmatic approach in the use of cloud storage. Cloud storage is simply a way in which to store data off site. Data is held on servers at various locations throughout the world. CWC purchase cloud storage within the UK and Amsterdam, ICT have not secured cloud storage outside of these areas.

Where a new application is required, a "cloud first" approach is taken. If a supplier cannot offer a cloud hosted system, resilience forms an essential part of the supplier offering, this will include, secureness of the solution, resilience options, cost and ease of use. ICT have an Azure cloud presence via MS, which has proven to be cost effective when measured against other options. CWC use secure cloud storage rather than simple cloud storage which provides protection whilst data is in transit and provides the ability to set policies and permissions for each storage area, to control who has access to specific data. With MS being a major player in the world of technology their security in this area is one of the most effective, thus offering confidence in this mode of operation. Data

encryption is a key feature of the MS offering, ensuring all data is fully encrypted, this safeguards data moves. By adopting this approach, data is unlikely to be penetrated.

Although encrypted information is not 100% uncrackable, decryption requires a huge amount of computer processing power, forensic software, and a lot of time, therefore this is considered a valuable and well protected mode of protection. ICT hold strategic meetings with MS each month, with Cyber security being a permanent agenda item. This equips ICT with a full understanding of future offerings, current issues and similar. MS offer flexibility and scalability to suit our business, meaning the authority is only paying for storage which is used, thus ensuring no wasted expenditure.

2.8 There are multiple articles around the safety of using cloud storage versus on prem storage, but in effect many of the risks remain the same. On prem storage is open to physical damage, risks may also include damage such as flood or fire, whereas cloud storage is generally well protected in relation to these types of issues and data is duplicated on different cloud servers, therefore the risk is well managed and appropriately mitigated.

2.9 Throughout May 2019, ICT have engaged with an external body to secure a "**Cyber Security Essentials Plus certification**". This external assessment and verification covers 5 key modules: Secure Configuration, Boundary Firewall and Internet Gateways, Access Controls and Privilege Management, Managing Patches and Malware protection.

The award of this certification will ensure the authority is recognised for their outstanding position and methodologies applied, in the way it manages Cyber Security, keeping the Authority safe as possible from Cyber-attacks.

3.0 Further actions

The future roadmap to ensure Cyber security is continually reviewed, includes but is not limited to:

- PSN (Public Services Network) annual testing, unless ICT pass this each year we are not permitted to operate (PSN compliance provides a report on the authority's security arrangements. It demonstrates that our organisation's security arrangements, policies and controls are sufficiently rigorous for us to interact with the PSN and those connected to it).
- PEN (Penetration) testing of new and existing systems, ensuring suppliers pass critical security tasks so that they can continue to provide their services via the CWC network.
- Cloud App technology, which notifies ICT immediately of activity linked to our network outside of the UK.
- Continued education of internal staff by initiating phishing campaigns, City People articles and similar.
- Continual training for security staff within ICT to ensure skills are kept up to date.
- Trialling of new software to enhance security whilst addressing new types of attacks which have been identified.
- Attendance at the newly formed regional Cyber group to share concerns, experiences and ideas.

- Attendance at high profile seminars where information and new technologies are shared. The Civil Contingencies Act 2004 requires the Council as a ‘Category 1’ responder to perform seven duties that seek to improve the resilience of the Council and our local community. One of these duties is to: “maintain plans for the purpose of ensuring, so far as is reasonably practicable, that if an emergency occurs the person or body is able to continue to perform his or its functions” (Civil Contingencies Act 2004, Section 2(1)c.)”