COTSWOLD
DISTRICT COUNCIL

AUDIT COMMITTEE **25TH JULY 2019**

AGENDA ITEM (9)

CYBER SECURITY UPDATE

Accountable Member	Audit Committee
Accountable Officer	Tony Oladejo ICT Audit & Compliance Manager / Data Protection Officer Tel: (01993) 861194 Email: Tony.oladejo@publicagroup.uk

Purpose of Report	The purpose of the report is to provide the Audit Committee with a Cyber Security progress over a 35 month period.
Recommendation(s)	**That the report be noted.**
Reason(s) for Recommendation(s)	To provide assurance to the Committee that there is Cyber security action plan in place with progress millstones and that Cyber risks are being managed and appropriate actions are being undertaken to mitigate cyber risks.
Key Decision	No
Recommendation to Council	No

Financial Implications	There is no direct financial implications
Legal and Human Rights Implications	None
Environmental and Sustainability Implications	None
Human Resource Implications	None
Key Risks	Failure to control and secure ICT systems and data against unauthorised access including Cyber-crime attack.
Equalities Analysis	Not required

Related Decisions	None
Background Documents	None
Appendices	**Appendix 'A'** - Extract from Publica ICT Services Risk Register

Performance Management Follow Up	None

Background Information

1. In the Cyber Security report presented to the Audit Committee on the 24th January 2017, we concluded that the ICT infrastructure is subject to ongoing and evolving cyber-attacks which, to date have been successfully rebuffed. It was recognised that the security infrastructure must continuously evolve to combat new threats and that the detection of Cyber incidents was as important as prevention.

2. The ICT team has merged the partner Council's networks and built resilience into the infrastructure whilst also implementing changes to the network as part of its overall strategy. In total, the team provides an ICT service across 29 sites within the four Partner Councils and three Clients (Ubico, Cheltenham Borough Homes and the Cheltenham Trust) serving more than 1,500 active users.

3. In preparation for a Cyber Security incident, we follow a Prevent, Detect & Recover multi-layer strategy with assurances sought for each stage. Our multi-layer strategy aligns with the Cabinet Office's UK National Cyber Security Strategy.

4. A recently published study on Cyber-attacks against government bodies highlights the importance of having resilient and robust arrangements in place fine, finding that:-

   - Local Authorities have experienced in excess of 98 million cyber-attacks over 5 years.
   - Approximately 150 councils experienced at least one cyber security incident - that is, an actual security breach - between 2013 and 2018.

5. This report outlines specific activities undertaken during a 35 month period: 1st February 2017 to 31st December 2019. Aimed at improving the Cyber security arrangements for all the organisations that the ICT team support and shows the forward plan in the tables below. The report does not include the names or the specifics of solutions used to prevent and detect Cyber incidents for obvious reasons.

Table 1 - Progress of specific Cyber Security activities over a 35 month period

Months	Key Cyber Security Activities	Status
Feb 17 to July 17	Introduction of ICT Policies Framework – The Framework consist of a number of operational Security Policies. Our policies are split into 'User' e.g. Password policy and Internal Operational polices such as Authentication and Patching procedures.	Completed
Aug 17 to Jan 18	We have introduced scan and Isolate capabilities. This system will constantly scan our IT infrastructure looking for systems that have been compromised and upon detection will isolate the offending system until remediation can take place.	Completed
Feb 18 to July 18	Spectre & Meltdown Virus - All devices in use by the partner Councils needed multiple patches, not just of software like Windows but also device firmware, BIOS & virtualisation layers. This consumed a great deal of the	Completed

	available resource.	
Aug 2018 to Jan 2018	Roll out of Next Generation Client Protection Software - All devices across the infrastructure were updated to include Next Generation Cyber Security Tools that actively look for suspicious behaviour. E.g. malware activities inside fraudulent invoices. In the past this protection was provided by Anti-Virus solutions that matched on files rather than behaviour. Cyber Essentials Plus Application process begins including onsite assessment	Completed
Feb 2019 To June 2019	Key Milestone: Cyber Essentials Plus achieved Changing our internal encryption cyphers (algorithms) to the latest standards to ensure compliance, in particular Payment Card Industry (PCI DSS) banking standards. New ICT Engineer dedicated to Cyber Security has been recruited Cyber Awareness training begins for all staff and continues throughout 2019 Internal Penetration Scan - external company works from within to scan all internal systems giving assurance as well as a list of vulnerabilities External Penetration Scan - external company attempts to break in externally and provide a report and list of vulnerabilities The Councils' LGA Cyber security funding bid was successful for its Cyber Resilience awareness programme PSN Code of Connection submitted to Cabinet Office's (PSN - Cyber Compliance Team). Liaison with PSN and Cyber Compliance team	Completed
July 2019 To December 2019	PSN assessment completed and certificate issued Completion of Cyber Awareness training	In Progress

6. Our Cyber Collaborations

6.1 We will also continue to expand our Cyber collaboration with external experts, these include:

- Zephyr Regional Cyber Crime Unit

The partner Councils have formally registered with the Zephyr Regional Cyber Crime Unit (RCCU). This provides a forum to receive and share up-to-date cyber threat information and the sharing of best practice.

- National Cyber Security Centre

ICT constantly review cyber security updates and guidance from Central Government's National Cyber Security Centre (NCSC), their remit is to provide support to public and private sector on how to avoid cyber threats

- Gloucestershire Local Resilience Forum (LRF)

The LFR provides a strategic cyber plan framework to all its partners to a known Cyber-attack. The key objectives are:

- Assist with the decision making process required to support a coordinated multi agency response to a Cyber-attack.
- Help gain a clear understanding of the potential impact and ongoing implications arising from a Cyber-attack.
- Develop a working strategy for the initial response phase.
- Consider how the current resilience arrangements are best utilised.

7. Conclusion

7.1 We have an assured, secure, government-accredited network. Progress has continued to be made on both our information security and Cyber Security arrangements, which should reduce the level of risk for the partner Councils and Publica.

There is a need to ensure focus on resilience against the threats of cyber-attacks are maintained and strengthened through organisation redesign, both at Council and Publica level to continue to mitigate the risks of authorised access and information loss.

(END)