Cheltenham Borough Council
Audit Committee – 23rd January 2019
Tony Oladejo ICT - Audit and Compliance Manager,

Accountable member	**Cabinet Member Corporate Services, Councillor Alex Hegenbarth**
Accountable officer	**Tony Oladejo**
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	The purpose of the report is to provide the Audit Committee with a Cyber Security progress update on the agreed action plans during 2018 and what activities are planned for 2019.
Recommendations	**That the Report be noted**

Financial implications	***None*** ***Contact officer: paul.Jones@cheltenham.gov.uk***
Legal implications	***None*** **Contact officer: Onelegal@tewkesbury.gov.uk**
HR implications (including learning and organisational development)	***None*** **Contact officer: Helen.chamberlain@publicagroup.uk**
Key risks	Failure to control and secure ICT systems and data against unauthorised access including Cyber-crime attack
Corporate and community plan Implications	**None**
Environmental and climate change implications	**None**
Property/Asset Implications	**None** **Contact officer: David Roberts@cheltenham.gov.uk**

1. Background

1.1 In the Cyber Security report presented to the Audit Committee on the 22nd March 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.

1.2 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 startegy. 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.

1.3 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.

1.4 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.
- 114 councils experienced at least one cyber security incident - that is, an actual security breach - between 2013 and 2017

1.5 This report outlines specific activities undertaken during 2018 aimed at improving the Cyber security arrangements for all the organisations that the ICT team support and shows the forward plan for 2019 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 - Summary of progress against agreed activities undertaken in 2018

Spectre & Meltdown Virus	January 2018 started with the news that every Intel processor in use across the world had a fundamental manufacturing flaw. Whilst most consumers continue to live with these vulnerabilities today, this was not acceptable for the Councils. All devices in use by the Council needed multiple patches, not just of software like Windows but also device firmware, BIOS & virtualisation layers. This consumed a great deal of the available resource.
External Penetration Scan & Health Check.	A full scan of all connection points to the network. We then create a mitigation plan to improve or plug any security weaknesses identified.
Internal Penetration Scans & Health Check	An external company was invited onto our premises and asked to attack the network as if they were an internal member of staff or someone with access to our buildings. The engagement was booked for 5 days and the first task is to break into the network without any assistance. After a day of trying, the company asked us to give them some basic user credentials to help them get started as there was a risk they would not complete the tests and produce the reports we needed within the timescales provided. A mitigation plan was created and actioned.
Roll out of Next Generation Client Protection Software	During 2018, 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.
LGA Cyber Security Stocktake - Individual Cyber Security Assessment	Submitted and Amber/Green rating received for Cheltenham. There is opportunity improve the council's cyber security arrangements by using this assessment to bid for future funding which is being looked at during 2019.
PSN Compliance Process	Completed successfully in June 2018.
Additional Staff Resources for Cyber Security	During 2018 it was recognised that we needed additional and up to date Cyber Security skills within the ICT team.
Implemented TLS 1.2 on all external payment devices	To remain compliant with the latest PCI-DSS standards a great deal of effort was put in to making sure that all external payment transactions were protected using SSL version 1.2. This included connectivity with HMRC.
Procurement of training software	Identified, selected and procured a Cyber Security training package to be used by all staff connected to the network.

Table 2 - Summary of specific activities planned for 2019 (some dates may change)

January 2019	Removal of TLS version 1.0 & 1.1 from internal Servers New ICT Engineer dedicated to Cyber Security starts work on 14th January
February 2019	External Penetration Scan booked - external company will scan all connectivity between the Councils & The Internet.
March 2019	Onsite Penetration Scan - external company works from within to scan all internal systems giving assurance as well as a list of vulnerabilities. These vulnerabilities will inform the Cyber improvement plan for the rest of 2019. Cyber Essentials Plus Application process begins including onsite assessment.
April 2019	PSN Submission Preparation Health Check Mitigation Begins
May 2019	PSN Submission Online Cyber Awareness & Information Security training to CBC staff
June 2019	Health Check Mitigation Completed

1.6 During 2018 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.

Over the past few years, Local Councils have relied on the PSN Code of Connection for external assurance. This year we are also including Cyber Essentials Plus.

- **Cyber Essentials Plus**

During 2017 the NCSC (National Cyber Security Centre) created the Cyber Essentials program. Details of which can be found here.

https://www.cyberessentials.ncsc.gov.uk/getting-certified/

This certification involves external security professionals testing our systems from the Internet and onsite before approving our infrastructure and associated systems.

- **Public Services Network Code of Compliance**

Public Services Network (PSN) provides an assured “network of networks” over which government and local authorities can safely share services.

2. CONCLUSIONS

2.1 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 is maintained and strengthened through organisation redesign, both at Council and Publica level to continue to mitigate the risks of authorised access and information loss.

Report author	**Contact officer: Tony.oladejo@publicagroup.uk**
Appendices	1. Extract from Publica ICT Services Risk Register