Cheltenham Borough Council

Audit, Compliance and Governance Committee – 22 January 2020

Cyber Security Update

Accountable member	**Alex Hegenbarth, Cabinet Member Corporate Services**
Accountable officer	**Tony Oladejo, Audit and Compliance Manager / Data Protection Officer**
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	To update the Audit Committee on the Cyber Security Action Plan in place, outlining the progress made against millstones to provide assurance that Cyber related risks are being managed and appropriate actions are being undertaken
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: Deborah.bainbridge@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: Dominic.stead@cheltenham.gov.uk**

1. Executive Summary

1.1 In the Cyber Security update report presented to the Audit Committee in January 2019, we concluded that the ICT infrastructure is subject to ongoing and evolving cyber-attacks which, to date and to the best of our knowledge 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 provides a service across 29 sites within the four Partner Councils including clients such as; Ubico, Cheltenham Borough Homes and the Cheltenham Trust serving more than 1,500 active users. Cyber & Information Security is at the forefront of all activities.

1.3 To enhance our resilience against a major cyber disaster, we currently adopt 'Prevent, Detect & Recover' multi-layer strategy with assurances sought for each stage. Our Cyber Security Action Plan aligns itself with the National Cyber Security Strategy. Our objective is to focus our resilience on prevention and detection activities against the threats of cyber-attacks through strengthened redesign and good preparation. By building understanding of cyber risks and threats, we can take the appropriate measures to stay safe but still take advantage of the benefits from working online.

1.4 As part of our ICT Business Continuity and Disaster Recovery programme to mitigate risks associated with other disaster scenarios, we continually select key disaster scenarios that may have the potential to disrupt our ICT services. This capability will be crucial in any Cyber Security incident.

1.5 We continually seek cyber security support and collaboration from partners such as the National Cyber Security Centre (NCSC). In a NCSC's recent Annual review 2019 , it highlighted:

- They assisted in more than 650 major cyber incidents
- They took down more than 170,000 malicious phishing URLs sites
- Awarded more than 14,000 Cyber Essential Certificates (including one to Cheltenham Borough Council)

1.6 This report outlines specific activities undertaken during 2019 aimed at improving the Cyber security arrangements for all the organisations that the ICT team support and shows the forward plan for 2020 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. We are happy to share more details in person with Audit Committee members if necessary.

1.7 The surge in the use of Software as Service (SaaS) and our users embracing flexible working from multiple devices in a variety of locations means our traditional network perimeter is disappearing and with it, the value of traditional defences.

1.8 One of our key risks in 2020 will be shadow ICT through the use of unauthorised cloud based software. Whilst this is actually an Information Security risk rather than Cyber Security risk it will be seen as a Cyber incident / breach. We mitigate these risks using the Cheltenham Technical Design Authority where all requests for Applications & Systems are reviewed.

1.9 Over the next 12 to 24 months we see us continue to move towards a 'Zero Trust' approach to our security architecture as championed and used by the NCSC, GCHQ and other similar organisations. This is achieved by building trust into the user's identity, their devices, and the services they access rather than the networks they connect to.

Table 1 – Progress of specific Key Cyber Security Activities over 12 month period:

Months	Key Cyber Security Activities	Status
Jan 19 to Mar 19	Cyber Essentials Plus Accreditation application process begins which includes onsite assessment by accredited security consultants. Changing our internal encryption cyphers (algorithms) to the latest standards to ensure compliance, in particular Payment Card Industry (PCI DSS) banking standards	**Completed**
April 19 to June 19	New ICT Cyber Engineer recruited Internal Penetration Scan - external company (accredited Crest & Check assessors) 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 Vulnerabilities mitigated and PSN Code of Connection submitted to Cabinet Office's (PSN - Cyber Compliance Team). **Key Milestone :** Cyber Essentials Plus accreditation achieved	**Completed**
July 19 to Sept 19	**Key Milestone** : PSN assessment completed and Certificates issued for all partner Councils The LGA Cyber security funding bid was successful for the Cyber Resilience awareness programme. This funding will help co-finance our Cyber security framework across the partner Councils Migration from Windows 2008 R2 Server (going end of life January 2020) continues.	**Completed**
Oct 19 to Dec 19	All ICT staff complete additional Cyber & Data Protection awareness training. End user device security software changed to different supplier providing additional detection and reporting capabilities. Migration from Windows 2008 R2 Server (going end of life January 2020) continues.	**Completed**

	Modified infrastructure to allow compatibility with Gov Wifi enabling the rental of the 2nd Floor at the Municipal Building.	

Table 2 - Summary of specific activities planned for 2020 (some dates may change)

Jan 20 to Mar 20	Review of ICT Policies Framework – The framework consists of a number of operational Security Policies. Deployment of an additional network based Intrusion Detection System. (IDS) PSN Submission process preparation Mitigation put in place for Windows 2008 R2 servers not upgraded. 10 Servers in total from the 300+ servers that run on the infrastructure across all partners Councils. Extended support contract agreed by working with Crown Commercial Services as used by Central Government and the NHS.
Apr 20 to Jun 20	Cyber Disaster recovery exercise Internal & External Penetration Scan work commences for annual PSN submission. PSN Submission Complete rollout of 802.1X authentication across the infrastructure.
Jul 20 to Sept 20	Phishing Simulations exercise
Oct 20 to Dec 20	Re-configuring on premise application servers to use the latest encryption ciphers available Investigate disabling weak authentication controls across the domain. Review service account permissions. Completion of online Cyber Awareness training to all CBC staff

1.10 During 2020 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 security updates and the use of cyber support tools 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

- **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 security infrastructure that is able to evolve as the organisation changes.

2.2 People and Human Behaviour is our greatest risk. Staff awareness around Information Security and good practice when using technology should continue to be mandatory for all employees.

2.3 Shadow IT in the form of unauthorised Cloud based software will continue to be a risk and it is important that Managers and Staff continue to send all requests to the Technical Design Authority for approval rather than "just signing up".

2.4 At some point in the future, the Council will be affected by a Cyber-attack. It is sadly inevitable. However when it occurs, our detection systems will enable us to choose the best recovery method and our disaster recovery systems will allow us to recover.

Report author	**Contact officer:** **Tony.oladejo@publicagroup.uk**
Appendices	n/a
Background information	n/a