EAST HERTS COUNCIL

PERFORMANCE, AUDIT AND GOVERNANCE COMMITTEE – 22 JANUARY 2019

REPORT BY SIMON RUSSELL – ICT STRATEGIC PARTNERSHIP MANAGER

JOINT ICT SERVICE CYBER SECUIRTY AND RESILIENCE UPDATE

WARD(S) AFFECTED: All

Purpose/Summary of Report

- Update on progress and plan to strengthen and improve cyber security and resilience of ICT provision across the council's shared IT service.

RECOMMENDATION(S) FOR Performance, Audit and Governance Committee: That:	
(A)	**Members are invited to review and comment on the report**

1.0 Background

1.1 Audit reports have shown that Cyber security and resilience is an area within ICT that has been neglected in the past and have put both councils at great risk of down time and cyber-attacks. This has been highlighted as high priority for the ICT team to target.

2.0 Report

2.1 Power resilience: Installation of generator has been followed by structural works to ensure that second data centre at Cavendish is fully protected. This work was scheduled to be completed over the weekend of the 8 December 2018.

2.2 Dark Fibre link: This link between the two data centres in Stevenage is vulnerable to be severed by road works, which has happened twice in recent months. ICT are in the process of tendering for a Microwave connection between both sites which will be constantly active removing this single point of failure. This should be installed in Quarter 4.

2.3 VDI desktop provisioning: Any server 'down time' planned or otherwise, causes serious disruption of the service as there is a delay in the provision of desktops to staff as they cannot be provisioned quickly enough. This is because of limitations of the present version of Horizon VDI and bottlenecks in the switches connected to them. The budget has been secured to update to the latest version of Horizon (7), update required storage and replace all switches across the network which are over 5 year old. Tender process is being started and we are anticipating installation in Quarter 1 2019.

2.4 Firewalls: All the council's firewalls are over 5 years with the exception of 2 which are 3 years old. A budget has been allocated to replace all firewalls during the financial year 2019/2020

2.5 Public Service Network (PSN): We are awaiting approval of our PSN certification. The external ICT health check showed 99 areas of high risk. Over the past few months these have been reduced that to 2 and expect resolution of those end of 2018.

2.6 Email security: We have setup TLS 1.2 and DMARC, this is ongoing work but allows us to discontinue the use of GCSX email which is ending operation in March 2019. Those emails

will be included in our ‘normal’ email setup in Exchange and the end result is a much higher level of security and encryption for all the council’s emails.

2.7 Unsupported Operating Systems: All unsupported OS and databases have now been removed from the council’s networks and we have started a scheme of work to remove Windows 2008 and SQL which will come out of support in 2019.

2.8 PSN Phase 2: We have started a scheme of work to focus on areas of vulnerability identified by PSN but which does not affect our ability to be certified.

2.9 Storage: Our present storage is 6 years old and the security firmware is not supported. Budget has been obtained to replace the storage in Q4/Q1.

3.0 Web and Email filtering: These systems are scheduled to be replaced during financial year 2019/2020

3.1 Office 365: Email and unstructured data will be transitioned to Office 365 as part of the move to cloud services. This brings with it in-built security features of the software but also other risks. As part of this solution we will be looking to implement two factor authentications.

3.2 ICT Staff restructure: The department is undergoing a restructure and as part of that, two new positions have been created: senior security and network technicians. These two positions will focus purely on securing and maintaining the security of the councils systems. At present this responsibility is spread across the IT team and thus has no real focus. The creation of these roles will resolve that issue and also enable the time resource to resolve and implement many of the systems and solutions aforementioned.

3.3 Data Compliance and GDPR: The data compliance team is to be moved into the ICT department from January 1st2019. At present this is just one permanent staff member and two temps, and discussions are being held about staffing. The proposal is to have joined approach to data protection and GDPR. Systems are being investigated to cover the governance side of GDPR.

4.0 Implications/Consultations

4.1 Information on any corporate issues and consultation associated with this report can be found within **Essential Reference Paper 'A'**.

Report Author: Simon Russell – ICT Strategic Partnership Manager
simon.russell@stevenage.gov.uk

Contact Officer: Name - Simon Russell – ICT Strategic Partnership Manager
simon.russell@stevenage.gov.uk