ITEM 11

REPORT TO: **WEST OF ENGLAND COMBINED AUTHORITY AUDIT COMMITTEE**

DATE: **09/12/2021**

REPORT TITLE: **CYBERSECURITY**

DIRECTOR: **MALCOLM COE – DIRECTOR OF INVESTMENT AND CORPORATE SERVICES**

AUTHOR: **CAROLINE PEGDEN – SERVICE LEAD, DIGITAL AND TECHNOLOGY**

Purpose of Report

1 To provide an update to the Audit Committee on the IT security controls implemented in light of the recommendations from Grant Thornton UK LLP.

Impact of Covid-19 pandemic

As a result of the Covid-19 pandemic, the majority of the Combined Authority's staff have been working from home for the past 20 months. The IT hardware, software and policies have been adapted to support remote working.

Recommendation

2 Members are asked to note the changes undertaken to enhance the Combined Authority's cyber-security and IT resilience.

Background / Issues for Consideration

3 **Context:** Following the change in outsourced IT supplier to Agilisys, the Combined Authority needed to update its IT security strategy and associated action plan. As detailed below, real progress has been made since the Grant Thornton Audit.

4 **IT Security strategy:** The Combined Authority has developed a new IT Security strategy following the National Cyber Security Centre's (NCSC) best practices, adapted to the Combined Authority's specific context, and validated at the Digital Board in July 2021.

5 **Turning the IT Security strategy into action:** The Combined Authority's Digital and Technology Service has then focused on turning this strategy into action, as illustrated below:

a. **Risk management:** Following the NCSC's best practices, the Combined Authority is following a risk-based approach to securing its data and systems.
   - **Cyber-security framework:**
     - Undertook our first IT Health Check, independently to North Somerset Council, in October 2020, in partnership with Agilisys and SureCloud, a CREST-approved provider.
     - Addressed all critical vulnerabilities which led to a number of security enhancements (e.g., WiFi monthly password changes, DKIM enhancements, ban of un-encrypted mass storage devices, introduction of multi-factor authentication for both internal colleagues and external guests).
     - Applied for our own Public Services Network connection compliance certificate in September 2021 *(waiting for feedback)*.
   - **IT risk register:** Created an IT risk register, to be reviewed quarterly.

b. **Engagement and training:** Flagged in the Grant Thornton report as an important area of focus, the Digital and Technology Service have worked on supporting our colleagues to obtain the skills and knowledge required to work securely. The team has focused on the following actions:

   - **Intranet:** Created a new ICT Security section on our Intranet with frequently asked questions, refreshed on a monthly basis.
   - **Awareness through our all staff communications updates:** Provided on-going ICT security updates on topical security issues, such as:
     - Phishing
     - Mass storage devices
     - Multi-factor authentication (MFA)
     - Benefits of using the Virtual Private Network (VPN)
     - Software upgrades.
   - **Training:** Focused on supporting our existing and new members of staff:
     - Delivered an ICT surgery on IT security.
     - Created a "New Starter Pack" including elements of cyber-security delivered to all new joiners.
     - Requested all new starters to complete the NCSC's e-learning course on essential cyber-security "Top Tips for Staff".
     - Upskilled the Service Lead, Digital and Technology and Workplace Support Manager when it comes to cyber-security.
   - **Policy updates:** Created a new "Digital Communications Policy" and "Information Technology Acceptable Use Policy", in partnership with HR, Legal and Communications:
     - to be signed off by all new colleagues as part of their induction checklist from December 2021 onwards,
     - to be signed off by all existing colleagues as part of the PDR process in January 2022.

c. **Supply chain / Asset Management and Data Security:** Defined new ICT security procurement criteria based on the NCSC's best practices and a risk-based approach, now available on our Intranet and shared with colleagues when they undertake procurement with a digital or technology component.

d. **Architecture & Configuration / Vulnerability management:** Working in partnership with Agilisys and other third-party suppliers to keep our systems and data protected throughout their lifecycle, and as new vulnerabilities emerge:

   - Promoted the use of the VPN and encouraged our colleagues to keep their devices updated *(on-going).*
   - Currently in discussion with Agilisys to introduce Azure Platform-as-a Service (PaaS) for our geo-spatial infrastructure, paving the way for future database projects, ensuring that our systems are built and maintained with good cyber-security baked in.
   - Beyond the routine patches and maintenance upgrades undertaken by Agilisys, undertaking a yearly cycle of penetration tests / ICT health checks *(the next ICT health check should be initiated in January 2022)*.

e. **Identity management:** Working with Agilisys to identify continuous improvements to control who and what can access our systems and data:
   - Completed the deployment of Multi-Factor Authentication (MFA) for all our internal colleagues and external Teams guests.
   - As much as possible, requiring the use of Microsoft Single Sign-On on all our WECA systems (e.g., Office 365, as well as Azure PaaS and Dynamics 365) and other third-party systems.
   - In partnership with Agilisys, enhanced our management of leavers.
   - In partnership with Agilisys, validated new principles of engagement of third-party suppliers when they require to access / connect to our core infrastructure and data.

f. **Logging & Monitoring / Incident management:** Working in partnership with Agilisys and third parties to ensure that the systems we use are able to detect incidents and security events, and that we have planned our response to cyber incidents in advance.

Consultation

6 Cybersecurity is an on-going process. A monthly security forum has been established with Agilisys to ensure that systems and processes are adapted as new vulnerabilities emerge, and the organisation continues to grow.

7 Expert advice from North Somerset Council has been sought, and the new IT Security strategy and progress update is currently being reviewed by OneWest, the Combined Authority's internal auditors, to look for continuous improvements. Initial recommendations should be provided on 23 November 2021.

Other Options Considered

8 Having already entered into a commercial agreement with Agilisys for the provision of ICT services, WECA could not consider any alternative options when it comes to cyber-security.

Risk Management/Assessment

9 ICT security risks are being addressed as a result of this report, and as part of the Combined Authority's on-going work in partnership with Agilisys and third-party suppliers to implement continuous improvements as new vulnerabilities emerge.

Public Sector Equality Duties

10 There are no equality implications arising as a result of this report.

Finance Implications, including economic impact assessment where appropriate:

11 There are no financial implications arising as a result of this report.

Legal Implications:

12 There are no legal implications arising as a result of this report.

Climate Change Implications:

13 There are no climate change implications arising as a result of this report.

Human Resources Implications:

14 There are no HR implications arising as a result of this report.

West of England Combined Authority Contact:
Any person seeking background information relating to this item should seek the assistance of the contact officer for the meeting who is Ian Hird / Tim Milgate on 0117 332 1486; or by writing to West of England Combined Authority, 3 Rivergate, Temple Quay, Bristol BS1 6EW; email: democratic.services@westofengland-ca.gov.uk