6. INTERNAL AUDIT – MONITORING REPORT 30th June 2018

REPORT OF: Audit and Risk Manager
Contact Officer: Gillian Edwards
Email: gillian.edwards@midsussex.gov.uk Tel: 01444 477241

Wards Affected: All MSDC Wards
Key Decision: No
Report to: Audit Committee
5th September 2018

Purpose of Report

1. The purpose of this report is twofold; to update the Committee on the progress of the 2018/2019 Internal Audit Plan and to report on the progress made in implementing previously agreed recommendations.

Recommendation

2. The Committee is asked to receive this report.

Background

3. Work Completed

No audits have been completed since the last report, as at 17th August 2018.

All outstanding work has been scheduled, which mainly relates to the Council's fundamental systems, for completion by 31st March 2019.

4. Work in Progress

The reviews in progress and other work that has been undertaken in the period are shown at Appendix A.

National Fraud Initiative (NFI) Data Matching – Update

Since the last meeting in July, details of outstanding matches have been passed to the Business Unit Leader, Revenues and Benefits who is exploring the possibility of using an external provider to assist in processing and investigating the matches identified in the NFI Data Matching exercise. This is ongoing and more information will be provided at the next Committee meeting in November 2018.

Additionally, a short review is currently being undertaken as part of the NFI Data Matching Exercise, where it appears that there may be more than one person resident at a property where Single Person Discount of 25% is being claimed. The outcome of this work will be reported at the next meeting in November.

5. High priority findings in this period

There were no high priority findings to report in this period.

6. Follow Up Audits:

The follow ups below have been completed since the last Audit Committee.

Income Collection Audit 2017/2018

During this review, it was agreed that the Council would consider insuring against cyber-attacks. The Head of Corporate Resources has considered advice from the Council's insurers and is satisfied that appropriate cover is in place.

Payroll 2017/2018

It was reported at the last meeting that reconciliations between the Payroll system and the Financial Management System (FMS) had not been completed for the period October 2017- January 2018.

It has now been confirmed that these reconciliations are up to date as at 31st July and we are currently reviewing this. We are advised that reconciliations will be prepared on a monthly basis.

Tech Forge

It was reported at the last meeting that a limited assurance was given for Tech Forge Financial Management System as insufficient testing had been undertaken to confirm that information raised on the Tech Forge module correctly interfaced with the Financial Management System. Since then, further testing has been undertaken and the Head of Corporate Resources has confirmed that the system is now working appropriately and will be used.

7. Member Action- Cyber Security

This summary was produced after a request from Councillor Andrew Lea was received at the meeting of the Audit Committee on 24th July 2018 where it was agreed that information would be provided to the Committee about cyber-attacks, what they are and the impact that they can have.

This summary is based largely on information gained from the Chartered Institute of Internal Auditors, which is the Audit and Risk Manager's professional body and the only professional association for internal auditors in the UK and Ireland. It is therefore the foremost authority on internal auditing.

The Oxford English Dictionary defines *cyber* as '**relating to or characteristic of the culture of computers, information technology, and virtual reality'**

The National Cyber Security Centre, which is part of GCHQ provides the following definitions:

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber incident

A breach of the security rules for a system or service - most commonly:

- Attempts to gain unauthorised access to a system and/or to data.

- Unauthorised use of systems for the processing or storing of data.
- Changes to a systems firmware, software or hardware without the system owners consent.
- Malicious disruption and/or denial of service.

Cyber security

The protection of devices, services and networks — and the information on them — from theft or damage

What are Cyber Attacks?

The National Cyber Security Centre, in its report entitled 'The cyber threat to UK business' published in May 2018 highlighted the major incidents in the year 2017/2018 as follows:

The major incidents in 2017 included:

1. Ransomware and distributed denial of service attacks
2. Massive data breaches
3. Supply chain compromises
4. Fake news and information operations

The first and second are most relevant to the Council at this time.

Ransomware

A global attack using ransomware known as 'WannaCry' was launched on 12 May 2017. payment to allow users access. This was the largest cyber-attack to affect the NHS in England, although individual trusts had been attacked before that date.

The Local Government Association reported that On 5 April 2016, a Council situated in the North of England was hit by a cyber-attack, being a piece of ransomware called TeslaCrypt which managed to get onto the council's network. Whilst virus protection measures were in place, they were bypassed by a member of staff googling the website and going through the

In addition, ransom Distributed Denial of Service (DDoS) attacks - where hackers threaten to conduct DDoS attacks unless a ransom is paid - have increased since mid-2017 when a South Korean web hosting company paid a ransom fee in Bitcoin equivalent to US$ 1 million.

In late 2017, the hacking group Phantom Squad targeted organisations in Europe, Asia and the US. They threatened financial institutions, hosting providers, online gaming services and Software-as-a-Service (SaaS) organisations and demanded a 're-instatement of services' payment in Bitcoin. The anonymity provided by virtual currencies like Bitcoin allow cyber criminals to conduct bold attacks and potentially make a profit.

Massive data breaches

The reported number and scale of data breaches continued to increase in 2017, with Yahoo finally admitting in October that all of its 3 billion customers had been affected by the 2013 breach.

The techniques used in most cases where data breaches have occurred due to cyber-attacks were reported as being not particularly advanced (including exploiting unpatched vulnerabilities and spear-phishing).

There are numerous documented further examples of data breaches caused by cyber-attacks, including a UK-based telecoms company who reported a cyber-attack to Action Fraud, when they discovered that data about individuals due for phone upgrades had been stolen. This case was triaged as a priority by Action Fraud and passed to the National Crime Agency, who liaised with NCSC to ascertain the most appropriate response and analyse the large datasets involved.

Cyber Attacks and Local Government

The National Cyber Security Centre advises that in cyberspace it is often difficult to provide an accurate assessment of the threats that specific organisations face. However, *every* organisation is a potential victim. All organisations have something of value that is worth something to others.

LocalGov, in an article written in February 2018, states that Big Brother Watch found local authorities face 19.5 million cyber-attacks per year and that 29% of councils had experienced at least one security breach between 2013 and 2017. Of the 25 councils who experienced a loss or breach of data due to a cyber-security incident, although 56% failed to report it the report said.

The report also found that three-quarters of local authorities do not provide mandatory cyber security training to staff.

How does the Council protect itself against cyber-attacks

The Head of Digital and Customer Service provided the following summarised description of the measures used by the Council to counter cyber-attacks.

While we experience daily attempts to infect our systems, to date we have prevented them with the measures we have in place.

Last year we experienced an attempt to infect our systems by the first version of the 'WannaCry' software and this was stopped at the infected machine. Data on the machine was restored from backups and further infections prevented.

MSDC has a shared Security Policy with partners on the CenSus network. It aims to provide a basis on which the Council can implement and maintain a secure environment for its information assets across its ICT estate. It encompasses multiple layers of protection including at the systems level, through data governance and through education, awareness and guidance.

The Council's Information Governance Officer and Infrastructure Manager are members of the NCSC and receive regular updates from them, which includes advice on attacks. We are also signed up to NCSC web check, which is part of the overall NCSC active cyber defence. This provides alerts if it notices anything wrong on the website.

Systems Level
The Council approaches network security in a holistic manner ensuring appropriate controls are applied both at boundaries between systems and within the network. The network is segregated from the internet via control barriers as needed with no direct routing between internal systems and external networks.

The Council protects its boundaries to the Internet, in particular from malware attacks. All information supplied to or from Council ICT systems will be scanned for malicious content. At the entry points to our network we are running a device which reads and checks emails for viruses and spam. This uses two different antivirus vendors to ensure coverage. It also has an element, installed late last year following the attempt to infect our systems, which scans for 'active' content that could encrypt a machine and strips this out or disables it. For Councillors on Office 365, there is an additional filter providing another antivirus check.

Each PC is patched regularly and automatically. We also use a current supported version of Windows with the appropriate patches. We are scoping a project to upgrade machines to Windows 10 to ensure that when Windows 7.1 goes out of support that we have a secure environment.

Data Governance

We have recently upgraded our Microsoft licencing to ensure data is classified for use in our new systems, enabling us to implement auto detection of sensitive data and prevent it from being accidentally sent to the wrong people. As we continue to work through our data, checking it against retention schedules we are also ensuring it is classified according to its sensitivity. These processes ensure we apply the appropriate data governance policies to the data according to its risk.

Where sensitive Council data or personal data is being shared with third parties it is encrypted in transit whether the data is being shared via a WAN (e.g. the Internet) or using removable media.

Education, Awareness and Training

The Council ensures that staff are well educated and takes steps to control social media malware attacks, phishing emails and similar attacks. Our current working practices include:

- Full set of Information Security policies
- Subject Access Request procedure
- Breach procedure
- A general privacy notice
- Basic information on what we do with data on forms where we collect personal information
- Online data protection training for staff

Additionally, we review malware protection logs to detect trends and changes in threat profiles and make appropriate adjustments and improvements as needed. For example, providing advice on the Council's intranet if we receive any phishing or spear phishing attacks as well as mailing staff to alert them.

Background Papers

- Internal Audit reports relating to 2018/2019
- Working papers relating to 2018/2019

Appendix A

Internal Audit Plan 2018/2019

Progress Report as at 17th August 2018

Audit	Audit Plan Year	Audit Opinion- Assurance	Number of High Priority Findings	Comments
A. Work Completed in the Current Period				
B. Work In Progress				
NFI Data Matching	2018/19			
Taxi Drivers	2018/19			
Follow Ups				
Payroll	2017/18			