INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Cyber Security Management
TO:	Head of ICT Services	**DATE:**	4 May 2021
C.C.	Chief Executive Deputy Chief Executive (AJ) Head of Finance ICT Infrastructure Manager Portfolio Holder (Cllr Day)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2020/21 an audit review of the Council's Cyber Security Management was completed in March 2021. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 Cyber Security is an increasingly relevant risk to the Council and the wider public sector. The WannaCry event from May 2017 is one such example, which caused widespread disruption through the use of a Ransomware attack, mobilised by the EternalBlue exploit.

2.2 Ransomware attacks encrypt the data on the target network, with the threat actors demanding a ransom to supply a code to unlock the encryption. EternalBlue was the mechanism that enabled the attack to propagate across a target network.

2.3 This audit was undertaken to ensure the security, integrity and availability of the Council's systems and data through the effective management of Cyber Security controls.

3 Scope and Objectives of the Audit

3.1 The objective of the report is to ensure the security, integrity and availability of the Council's systems and data through the effective management of Cyber Security controls.

3.2 Testing was performed to confirm that controls identified operated as expected with documentary evidence being obtained where possible, although

some reliance has had to be placed on discussions with relevant staff. A maturity assessment approach was adopted for the testing.

3.3 The audit was designed to assess and provide assurance on the risks pertaining to the following key areas:

- Secure Configuration
- Malware Prevention
- Monitoring; and
- Home & Mobile Working

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as this is the first audit of this area.

4.2 Secure Configuration

4.2.1 We have noted that there is a documented Patch Management policy, which has undergone a recent review in February 2021. The policy covers patching across the infrastructure as well as the standard Windows patching processes for devices such as servers and user machines.

4.2.2 There are processes in place to ensure that all relevant Windows devices are patched as required, with other devices such as network switches and firewalls being patched as new updates are available. These are issued on a less frequent basis.

4.2.3 There are documented build sheets in place. These are used as a checklist to ensure that all new devices are set up in a consistent manner and that they have the required 'core' software installed. Such software includes Office products as well as Anti-Virus/Malware Endpoint Protection systems.

4.2.4 We have noted the presence of a range of other policies that help manage the secure configuration of the Council's systems. These include the Change Management policy, although the policy was noted as having been previously reviewed in May 2018.

Risk

Where a regular policy review is not undertaken, there is a risk that the policy does not stay aligned to any process changes that may be being implemented over time.

Recommendation

Regular reviews of the ICT Services – Change Management Policy should be conducted with the first one being as soon as possible.

4.2.5 The Council does not currently have a process in place whereby periodic vulnerability scans are carried out in addition to the annual mandatory Public Sector Network (PSN) External Penetration Test and Internal Health Check.

Advisory

Consideration should be given to the procurement of an appropriate internal vulnerability scan tool to facilitate the implementation of periodic internal vulnerability scans. Tools such as Tenable Nessus are available for such activities.

4.2.6 The support lifecycle of the Council's infrastructure is monitored on an ongoing basis and we have noted that there is a contract with a Third party contractor who provide advice and guidance for the management and procurement of this. Lifecycle management is vital to ensure that the Council only uses equipment that is supported by the relevant vendor and that replacements are planned in advance of support being withdrawn. Unsupported equipment will not receive new patches to deal with known vulnerabilities that may be exploited by threat actors.

4.3 Malware Prevention

4.3.1 We have noted the presence of a documented "Major Virus Outbreak procedure" and a "Removable Media Policy". However, these documents require review as they were last updated in 2016 and 2019 respectively.

Risk

Where regular policy reviews are not undertaken, there is a risk that they do not stay aligned to any process changes that may be being implemented over time.

Recommendation

Regular reviews of the "Major Virus Outbreak procedure" and "Removable Media Policy" should be conducted and communicated accordingly with the first ones being as soon as possible.

4.3.2 The Council's devices have appropriate Malware prevention systems in place that scan all data "on access", which means that data cannot be processed until a successful scan of it has been undertaken first. This is especially important where external data has been received, but is also important for internal data.

4.3.3 We have seen that the Council has a documented procedure for scanning external media such as CD-ROMs. This procedure is available as staff guidance in the event that media is received from external parties.

4.3.4 The Council has implemented a process whereby USB devices are blocked from being used and that users are restricted from downloading certain file types from the Internet.

4.3.5 Sophos Endpoint Protection monitors the compliance status of all relevant Council devices under its management. Compliance status relates to the currency of the signature files that are the virus updates to cater for the latest known vulnerabilities.

4.3.6 We have noted that the Current Sophos has about two years remaining on the contract. ICT Management have stated their intention to remain with Sophos, although remain mindful of alternative options.

4.4 Monitoring

4.4.1 The Council does not have a documented Network Monitoring policy and procedure in place. The policy and procedure sets out the scope of the monitoring processes and how to implement the processes.

Risk

Where there is no formal Network Monitoring Policy and Procedure in place, there is a risk that potential malicious and/ or inappropriate network activity goes undetected.

Recommendation

A formal Network Monitoring Policy and supporting operational procedures should be documented. The policy should set out the scope of the monitoring activity; for example, specifying the infrastructure logs that are relevant, roles and responsibilities and the reporting and follow up processes needing to be carried out.

4.4.2 However, we have noted that there are a range of operational monitoring systems in place, including the FirePower Intrusion Prevention System (IPS), the Cisco Prime Infrastructure monitoring dashboard and the VSphere Virtual Machine monitoring processes. The monitoring includes alerts that require attention or are for information purposes only.

4.4.3 The Council uses the services of British Telecom (BT) where incidents that require their assistance is required. BT provides support for the Council's Cisco infrastructure (primarily network devices and telephony) and advise on infrastructure changes.

4.5 Home & Mobile Working

4.5.1 The Council has documented a range of policies and related procedures that cover this space, including the management of Third party access to the Council's systems. The policies are as follows:

- Third Party Network Access Agreement
- Third Party Connection Policy
- Third Party Network Access Request form
- Third Party Remote Access Procedure; and
- Remote Working Policy for Staff and Members.

4.5.2 We have noted that all of these documents are outdated, having been last reviewed in 2018 and 2019.

Risk

Where regular policy reviews are not undertaken, there is a risk that they do not stay aligned to any process changes that may be being implemented over time.

Recommendation

Reviews should be conducted of the relevant Third Party remote access policies, their related procedures and the remote working policy for staff and members. A regular review of the policies should be undertaken on an appropriately regular basis.

4.5.3 The Council uses the Cisco AnyConnect Secure Mobility Client software to manage its remote access service. The service is supplemented by Multi-Factor Authentication.

4.5.4 We have noted that posture checking has also been implemented. Posture checking is a process whereby Council devices that are scanned to confirm that they comply with a minimum standard of rules before access to the Council's network is granted. The rules at the time of the audit were as follows:

- Client Anti-Virus signature files are no more than 15 days old
- The Windows 10 Operating system build is build 1803 or higher
- The posture checking process searches for a specific entry within the Windows registry that confirms it as a Council machine**.**

4.5.5 The posture checking was a recent change following a migration from VMWare Horizon to Council-managed devices with AnyConnect VPN. VMWare Horizon has been used as the remote working tool prior to the Pandemic. However, it was found that it was not suitable for supporting the sustained increase in demand for remote working, especially where telephony support is concerned.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did, however, identify four Low-rated issues which, if addressed, would improve the overall control environment. These are set out below:

- A need to conduct a review of the ICT Services – Change Management Policy and to ensure that a regular review of the policy is undertaken on an appropriately regular basis.
- A need to conduct reviews of the "Major Virus Outbreak procedure" and "Removable Media Policy".
- A need to document a formal Network Monitoring Policy and supporting operational procedures with the policy setting out the scope of the monitoring activity.
- A need to conduct regular reviews of the relevant Third Party remote access policies, their related procedures and the remote working policy for staff and members.

Consequently, the findings are considered to give SUBSTANTIAL assurance around the management of Cyber Security risks.

5.1 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

5.3 A further 'issue' was also identified where an advisory note has been reported. In this instance, no formal recommendation is warranted as there is little risk if the action is not taken.

6 Management Action

6.1 The recommendations arising above, are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Cyber Security Management – March 2021

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.4	Regular reviews of the ICT Services – Change Management Policy should be conducted with the first one being as soon as possible.	Where a regular policy review is not undertaken, there is a risk that the policy does not stay aligned to any process changes that may be being implemented over time.	Low	Head of ICT Services	A number of ICT's key operational policies have not been reviewed according to the normal schedules, principally due to the impact of COVID-19 on capacity to carry out the work and the absence of key staff within the service. The Change Management Policy will be reviewed to ensure that it includes key principles from the ITIL change management framework.	30/06/21

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.1	Regular reviews of the "Major Virus Outbreak procedure" and "Removable Media Policy" should be conducted and communicated accordingly with the first ones being as soon as possible.	Where regular policy reviews are not undertaken, there is a risk that they do not stay aligned to any process changes that may be being implemented over time.	Low	Head of ICT Services	A number of ICT's key operational policies have not been reviewed according to the normal schedules, principally due to the impact of COVID-19 on capacity to carry out the work and the absence of key staff within the service. The overall incident management policy and procedure, which includes the major virus outbreak procedure will be reviewed to ensure that it includes the latest guidance from NCSC. Removable media will also be reviewed as significant changes to its usefulness have taken place.	30/06/21

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.1	A formal Network Monitoring Policy and supporting operational procedures should be documented. The policy should set out the scope of the monitoring activity; for example, specifying the infrastructure logs that are relevant, roles and responsibilities and the reporting and follow up processes needing to be carried out.	Where there is no formal Network Monitoring Policy and Procedure in place, there is a risk that potential malicious and/ or inappropriate network activity goes undetected.	Low	Head of ICT Services	ICT can review its network monitoring and logging processes in line with the latest guidance from NCSC. An appropriate policy and process will be produced for consideration by the ICT Steering Group.	30/09/21

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.2	Reviews should be conducted of the relevant Third Party remote access policies, their related procedures and the remote working policy for staff and members. A regular review of the policies should be undertaken on an appropriately regular basis.	Where regular policy reviews are not undertaken, there is a risk that they do not stay aligned to any process changes that may be being implemented over time.	Low	Head of ICT Services	A number of ICT's key operational policies have not been reviewed according to the normal schedules, principally due to the impact of COVID-19 on capacity to carry out the work and the absence of key staff within the service. The Council's overall remote working and access policy requires a review to ensure that it takes account of the changed circumstances of WDC, where more staff are working remotely than ever before. A review of supplier remote access will also be undertaken to ensure that appropriate safeguards are in place and effective monitoring is operational.	30/09/21

* Risk Ratings are defined as follows:
High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.