INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Cyber Security
TO:	Deputy Chief Executive (AJ)	**DATE:**	16 March 2018
C.C.	Chief Executive Head of Finance ICT Services Manager Portfolio Holder (Cllr AM)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2017/18 an audit review of cyber security controls was completed in March 2018. 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 This audit was undertaken to review whether adequate Cyber Security processes and controls have been implemented in order to provide adequate protection to the Council network domain.

2.2 Cyber security processes and controls are intended to provide a minimum baseline of security in protecting the business against cyber threats such as malware or an external attack compromising the Council's data, systems or services.

3 Scope and Objectives of the Audit

3.1 The objective of the audit was to perform a review of the level of control in place to offset the ongoing threat of cyber-attack, taking into consideration the guidelines detailed as part of the Government's Cyber Essentials Scheme (CES).

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

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

- Firewalls and internet gateways;
- Secure configuration;

- Access control;
- Malware protection; and
- Patch management.

4 Findings

4.1 Recommendations from Previous Report

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

4.2 Policies & Procedures

4.2.1 The ICT policies and procedures relevant to the management of cyber security risks were identified and obtained during the review. These were used in the process of reviewing the suitability of the controls in in operation at the Council.

4.2.2 Policies identified as being of particular relevance to this review are as follows; Information Security and Conduct Policy, Patch Management Policy, Computer Security Policy, Removable Media Policy, and the Data Handling Policy.

4.2.3 ICT policies are made available to all staff via the Council's intranet. Key messages from the policies are included in the mandatory online training packages that are completed by all staff as part of the Council's induction process.

4.2.4 Policies were found to be subject to regular review and revision on at least an annual basis. It was noted that the Computer Security Policy and Data Handling Policy were being reviewed and updated at the time of this audit.

4.2.5 The policies reviewed were found to include sections for version control, a revision history and details of the relevant ICT staff who own and are accountable for the policy.

4.3 Firewalls & Internet Gateways

4.3.1 ICT has recently completed an exercise of updating and replacing the firewall infrastructure in use at the Council and are now using the Cisco Adaptive Security Appliance (ASA) as the main firewall solution. It was confirmed during the audit that this is the most up-to-date version and is actively supported by the supplier.

4.3.2 Access to the Council's firewalls is restricted to a limited number of approved ICT users only, with access restricted by IP address, user name and password.

4.3.3 Review of security settings on the main internal and external firewall identified that that, while the system requires the use of passwords that are eight characters or more, there are no other complexity requirements, such as a requirement that uppercase, lower case and numeric characters are used, currently enforced by the system.

Risk

Weak, insecure or non PSN compliant passwords may be used for administrator level activities.

Recommendation

ICT should review firewall password security parameters and ensure that all administrator password settings meet the Council's requirements around complexity.

4.3.4 It was noted through review of firewall rulesets that there are some legacy firewall rules in place for which the function and purpose is not immediately obvious from the detail provided. It is understood from subsequent discussions with ICT management that there are likely to be a number of firewall rules that are no longer used or required.

4.3.5 As the recently upgraded firewall platform provides improved reporting, including detail on how frequently firewall rules are used, it is recommended that this facility is used as part of a regular exercise to review firewall rulesets to ensure that that all rules are valid and that any unnecessary rules have been removed.

Risk

Unnecessary or incorrectly configured firewall rules may permit unauthorised access to Council systems or services in the event they are misused.

Recommendation

ICT should perform an exercise of reviewing and validating firewall rulesets. This should be performed on an at least annual basis to ensure firewall rules remain appropriately configured.

4.4 Secure Configuration

4.4.1 An annual exercise of vulnerability scanning and penetration testing is undertaken as part of the annual IT Health Check (ITHC) exercise required as part of the PSN accreditation process. This is used as means of verifying whether the Council's network is adequately protected against known vulnerabilities. Actions resulting from this ITHC report are logged and tracked to completion using an actions log.

4.4.2 Additional ad hoc vulnerability scanning and penetration testing exercises are performed in conjunction with third party consultants on a risk basis, where deemed necessary throughout the year.

4.4.3 A review of the actions identified as part of the last ITHC exercise identified that significant progress has been made in resolving / mitigating the issues identified but, at the time of audit, there were five 'High' and four 'Medium' rated issues that remained to be fully resolved or mitigated.

Risk

Known vulnerabilities may be exploited impacting the confidentiality, availability and / or integrity of Council data and systems.

Recommendation

ICT management should aim to resolve / mitigate remaining issues in order to help ensure PSN certification is retained.

4.4.4 It was noted that the Council does not currently make use of an active Intrusion Detection system, however it is understood that management were actively investigating options for this at the time of audit.

4.5 **Access Control**

4.5.1 It was noted through review of the ITHC action plans that there is an ongoing issue with the use of a standard local administrator username and password for a number of key Council servers.

4.5.2 It is understood from discussion with ICT management that resolving this issue presents difficulties in terms of managing the required number of unique passwords, and that the current approach of using Sharepoint to store password data is not ideal as key passwords would potentially be unavailable in the event of a disaster recovery situation.

Risk

With knowledge of the current admin username and password an attacker may be able to connect to multiple servers as well as accessing local drives.

Recommendation

ICT management should perform an exercise to review the approach to administrator passwords, including investigation into the use of a software solution.

4.5.3 A review of access permissions to firewall devices identified the existence of a default / generic administration level account on the main external firewall. It is understood that this is not actively used, but it is recommended that this is reviewed and deleted if possible to remove the potential for misuse.

Risk

The existence of a generic shared administrator accounts increases the risks around lack of accountability for any changes to firewall rules using the account.

Recommendation

ICT management should ensure that the generic administrator account is disabled and replaced with individually named administrator accounts.

4.6 Malware Protection

4.6.1 The Council uses a variety of solutions for antivirus / malware prevention and detection, with Sophos being the main system in use. Virus protection controls are deployed at the internet / network gateway level, at the network and server level, and on individual laptop and desktop machines.

4.6.2 Internet gateway controls include:

- perimeter located SPAM detection (used to reduce the risk of virus infected e-mails reaching the Council's e-mail server);
- antivirus solutions from two separate vendors (Kaspersky & Sophos) are used to scan inbound e-mail traffic;
- an internet proxy is used to restrict staff access to unauthorised or high risk sites.

4.6.3 Sophos features a high level dashboard enabling ICT to quickly identify any issues such as errors in updating antivirus definitions. Updates to antivirus definitions are deployed centrally, with checks for new updates performed every ten minutes.

4.6.4 ICT management has set up alerts within Sophos to notify them in the event Sophos is down, or in the event updates are not available. A weekly report is generated by the system detailing all antivirus events such as any positive detections.

4.6.5 It was noted that ICT management has recently implemented an anti-ransomware/ exploit prevention system, Sophos EXP, in order to minimise the potential for ransomware attacks impacting the Council's network.

4.6.6 It was found that this is currently in place and operating on approximately 98% of the Council's servers. It was noted that there is an ongoing issue with installing the system in the case of the ANYA2 server, and that there are two servers where the system has not yet been installed due to concerns from the business around the potential impact.

Risk

Unprotected servers may be vulnerable to the risk of a ransomware attack.

Recommendation

ICT should liaise with Sophos to identify and resolve the ANYA2 server issue and with business system owners to ensure the remaining servers are updated with Sophos EXP.

4.7 Patch Management

4.7.1 The Council's approach to patch management is documented in the 'Patch Management Policy'. Both automated and manual patching processes are in use and vary depending on the system / device being patched.

4.7.2 The key method of managing server, desktop, and application patching is via the use of Microsoft Windows Server Update Services (WSUS) which allows ICT to deploy the latest Microsoft product updates to computers running the Windows operating system. This is integrated into Microsoft's System Centre Configuration Manager (SCCM) which enables the automated delivery of patches.

4.7.3 A report detailing patching compliance for servers and workstations is automatically generated by the SCCM system. These reports allow ICT to gauge overall compliance against the list of deployed updates and are used to identify individual systems or devices that are not compliant.

5 Conclusions

5.2 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did identify four Medium and two Low rated issues which, if addressed, would improve the overall control environment. As a result the findings are considered to give SUBSTANTIAL assurance around the management of cyber security risks.

5.3 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.

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 – March 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.3	ICT should review firewall password security parameters and ensure that all administrator password settings meet the Council's requirements around complexity.	Weak, insecure or non PSN compliant passwords may be used for administrator level activities.	Low	ICT Infrastructure Manager	Accepted – The current password does meet the Council's password complexity standard, although it is accepted this is not enforced through the software control. The complexity parameter will be set.	April 2018
4.3.5	ICT should perform an exercise of reviewing and validating firewall rulesets. This should be performed on an at least annual basis to ensure firewall rules remain appropriately configured.	Unnecessary or incorrectly configured firewall rules may permit unauthorised access to Council systems or services in the event they are misused.	Medium	ICT Infrastructure Manager	Accepted – Sufficient data needs to be gathered to ensure that the deletion of a rule does not impact on the business. Once the data is gathered, legacy rules will be deleted and this will become an annual housekeeping task.	September 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.3	ICT management should aim to resolve/ mitigate the remaining ITHC issues in order to help ensure PSN certification is retained.	Known vulnerabilities may be exploited impacting the confidentiality, availability and/ or integrity of Council data and systems.	Medium	ICT Services Manager	The current ITHC reflected the security position 12 months ago. A new ITHC will take place w/c 19 March 2018. This will supersede the existing ITHC. ICT will, as per normal practice, evaluate and remediate as appropriate.	Complete – No further Action
4.5.2	ICT management should perform an exercise to review the approach to administrator passwords, including investigation into the use of a software solution.	With knowledge of the current admin username and password an attacker may be able to connect to multiple servers as well as accessing local drives.	Medium	ICT Infrastructure Manager	Accepted – A new approach to admin passwords has been agreed and will be rolled out to all servers. The new approach removes the need to invest in a software solution.	Complete – No further Action
4.5.3	ICT management should ensure that the generic administrator account is disabled and replaced with individually named administrator accounts.	The existence of a generic shared administrator accounts increases the risks around lack of accountability for any changes to firewall rules using the account.	Medium	ICT Infrastructure Manager	Accepted – The generic admin account has been disabled.	Complete – No further Action

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.6.6	ICT should liaise with Sophos to identify and resolve the ANYA2 server issue and with business system owners to ensure the remaining servers are updated with Sophos EXP.	Unprotected servers may be vulnerable to the risk of a ransomware attack.	Low	ICT Infrastructure Manager	Accepted – The ultimate resolution of this problem is outside the control of ICT Services. However, as per the recommendation, a support case has been raised with Sophos and will be followed through to conclusion.	Complete - No further Action

* 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.