Cyber Security

Peak District National Park Authority

Internal Audit Report 2020/21

Business Unit: ICT
Responsible Officer: Head of Information Management
Service Manager: IT Manager
Date Issued: 19 April 2021
Status: Final
Reference: 69200/001.bf

	P1	P2	P3
Actions	**0**	**0**	**1**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Organisations such as the Peak District National Park Authority (PDNPA) are increasingly reliant on technology to store and use data. Therefore it is essential that there are comprehensive security measures in place that help ensure data, systems and assets are protected from damage, unauthorised access, loss and misuse.

Ransomware has recently become significantly more prevalent. Since August 2020, the National Cyber Security Centre (NCSC) has investigated an increased number of ransomware attacks in the UK. Implementing secure email security controls and access controls is a way of reducing the risk of ransomware along with other types of malware.

The security of applications is a growing concern as these are used to store sensitive data and facilitate some key functions. It is key to ensure there are management controls in place to ensure data held within the applications is secure.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- Arrangements are in place to ensure that the required security configuration will be applied to email communications and other security measures, such as the checking of email authenticity, are in place and operating effectively.
- Access controls are appropriately authorised and monitored.
- Applications configurations have been hardened, changes to applications go through strict change management controls and actions are logged.

Key Findings

We compared the PDNPA's emails security configuration with the NCSC's malicious email strategies guidance. The guidance split their recommendations in to four categories; minimal, average, good and excellent security effectiveness. The Authority has a strong email security configuration in place and complied with all the recommendations apart from a couple of areas within the excellent category.

The Authority has a blacklist of prohibited file types, but does not have a whitelist of acceptable file types. The NCSCS recommend whitelisting as it is more proactive and thorough than blacklisting, and it ensures only specified file types can be received while others are blocked. However, currently the Authorities email system supplier does not allow for a whitelist. Email are from outside sources containing attachments are scanned for malicious content. A plugin on the anti-virus software decrypts messages scans them and encrypts it again. If the anti-virus software cannot decrypt the message it is then flagged as spam.

The Authority has a clear process within the starters and leavers policy to ensure that IT is updated when new members of the authority have joined and when individuals leave. Inactive user accounts are reviewed by IT. We verified that there was no individuals who have left the authority that still have access to the network. The active directory domain controller settings complied with ISACA's Active directory guidance.

Privileged user accounts are segregated from other user accounts and they are only used for administering purposes. Users are unable to login to the authority's network remotely on non PDNPA device. This greatly mitigates the risk of unauthorised gaining access to the network, although the current minimum password standards do not comply with the latest guidance.

Minimal changes to the authorities applications have been made during the year however all changes are logged. Applications are configured within a secure manner. The internal network undergoes periodic penetration testing following any changes to the network. The Authority have also commissioned penetration tests of their web applications. The authority has addressed the issues that was identified by the tests. All changes to applications are logged.

Overall Conclusions

A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Passwords

Issue/Control Weakness	Risk
The authority's minimum password requirements does not meet best practice.	Unauthorised access to the network.

Findings

Password can easily be stolen by cyber criminals. The use of 2 factor authorisation provides additional security against cybercrime. There are a number of types of two factor authentication available. Authenticator applications that are synced with the users account can be installed on a user's phone and provides a separate code for each log in. Alternatively, the method used at the PDNPA is that the users PDNPA device is linked to their Active directory account. Access to their user account can only be gained if they are using their predetermined work provided device.

The NCSC recommends that organisations should implement a minimum password length but does not specify what the minimum length should be. Whereas the US National Institute of Standards and Technology (NIST) recommend password length should be a minimum of 8-64 Characters. Microsoft recommend keeping minimum password length of 8 as password length requirements (greater than about 10 characters) can result in user behaviour that is predictable and undesirable. For example, users who are required to have a 16-character password may choose repeating patterns like fourfourfourfour that meet the character length requirement but are not difficult to guess.

The authority's minimum password length is seven Characters in length This is below the NIST and Microsoft recommended minimum length

Agreed Action 1.1

Password policy minimum password length to be changed to 8 characters.

Priority	3
Responsible Officer	IT Manager
Timescale	31 July 2021

Audit Opinions and Priorities for Actions

Audit Opinions	
Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit. Our overall audit opinion is based on 4 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.

PEAK DISTRICT NATIONAL PARK