THE CHIEF CONSTABLE OF NORTH YORKSHIRE

Cyber Risk Management

Internal audit report 9.21/22

FINAL

30 May 2022

1. EXECUTIVE SUMMARY

Why we completed this audit

We have undertaken an audit to provide assurance that computer systems and data at the organisation are resilient to threats resulting from connection to the internet.

In the past 18 months, we have seen the cyber-crime threat landscape amplified by the impact of the COVID-19 pandemic as cyber criminals seek to capitalise on the disorder. Our recent 2021 survey highlighted that 20 per cent of organisations had experienced a cyber-attack over this period, with 71 per cent stating the attack was a direct result of the coronavirus pandemic (https://www.rsmuk.com/real-economy/cybersecurity).

The audit scope focussed on certain controls related to secure configuration, vulnerability management, incident management, and monitoring. Specifically excluded from the scope of this review was the following cyber areas; Risk management, Engagement and training, Asset management, Architecture and configuration, Identity and access management, Data security (data classification and backups), and supply chain security.

The audit was carried out through virtual meetings, review of key documentation and sample testing relevant to the scope of the audit.

Conclusion

There has been a focus from the Force over the past 12 months to improve their cyber security posture and reduce their cyber risk exposure by establishing policies and managing the IT estate. Good practice identified during our review includes an intrusion prevention capability, monitoring and alerting processes, and oversight from the Senior Leadership Team of the organisation's vulnerability and patch management positions through reporting. Management is also aiming to achieve Cyber Essentials Plus accreditation in 2022.

Whilst good practice has been identified in each scope area, there have also been weaknesses/gaps identified in each of these areas which requires management attention. The detailed findings and actions section provides further detail on the management actions agreed as part of our review which comprise of **five medium** and **one low** priority management actions.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of North Yorkshire can take **reasonable assurance** that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.

Key findings

Our audit identified the following exceptions resulting in five medium priority management actions being agreed:

Windows patching is in place, however, there are devices running end of life Windows 10 versions and, as such, there is a risk that vulnerabilities exist on these devices which cannot be patched. **(Medium)**

A Vulnerability and Patch Management Policy is in place however, it does not include information such as testing requirements, roles and responsibilities, and the deployment process. Without a more expansive policy in place, there is a risk of mismanagement of vulnerabilities and patches as the direction and strategy is not clear and cannot be referenced by staff. **(Medium)**

A patch management process is in place, however, there are servers in the IT estate requiring updates which creates a risk of servers currently operating with known or unknown vulnerabilities. **(Medium)**

A vulnerability management process is in place with reporting to the leadership team, however, there are outstanding critical vulnerabilities in the IT estate which could be exploited. The list of potential critical vulnerabilities had reduced from 86% to 12%, as per the latest management reports, and therefore we are satisfied this is receiving management attention. However, this issue still needs further work to minimise risk even further. **(Medium)**

An intrusion detection system is in place however it is not being utilised. If intrusion detection is not fully utilised, there is a risk that potential security events are not identified. **(Medium)**

For details of the remaining **one low** priority action, please see section two of this report.

Our audit review also identified that the following controls are suitably designed, consistently applied, and are operating effectively:

Management evidenced the intrusion prevention capability in place through their firewall platform which allows for potential malicious activity on the network to be blocked.

We received evidence showing windows patches being tested through deployment to smaller pre-release test groups before deployment to the wider IT estate which reduces the risk of operational disruption or introduction of vulnerabilities into the IT estate.

We reviewed evidence of communications that were sent out to users in response to upcoming changes that may impact them which helps reduce operational disruptions.

A change management process is in place and followed during patch and vulnerability management processes which was evidenced through examples of a standard, normal, and emergency change. This reduces the risk of operational disruption and introducing vulnerabilities into the estate.

Evidence was provided showing account monitoring and alerting capability through summary reporting from the National Monitoring Centre (NMC) as well as alerts in response to specific incidents such as multiple login failures for a single username. These controls reduce the risks associated with compromised accounts.

Annual IT health checks are completed and were evidenced along with the remediation plan which is approved by Senior Information Risk Owner. The identification and remediation of vulnerabilities will help reduce the organisation’s risk exposure.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Risk: Risk reference: 8004				
Control	Windows patches are automatically deployed every month.	**Assessment:**		
		Design	✓	
		Compliance	×	
Findings / Implications	We received a breakdown of the number of Windows version installations across the devices. The first screenshot received in December 2021 showed compliance for the installation of Windows at 20 per cent (835 installations across 4,218 devices). However, on review of the breakdown, there were devices that were running end of life Windows 10 versions: • vabc – 174 (4 per cent) – end of life 8 October 2019; • vdef – 1 (<1 per cent) – end of life 8 December 2020; and • vxyz – 3202 (76 per cent) – end of life 11 May 2021. On discussion with management, the reason for devices largely running end of life versions of Windows was stated as primarily due to the release of various National Enabling Programme blueprints, the replacement of the senior management structure, the integration of North Yorkshire Fire and Rescue Service and Covid-19. An updated screenshot was received in February 2022 which showed that the installations of Windows had increased to 26 per cent (1,098 installations across 4224 devices) and management aim to have the majority of devices completed by June 2022. However, as long as devices in the IT estate are running end of life versions of Windows 10 there is a risk that vulnerabilities exist on devices which cannot be patched and so, if exploited, could lead to a data breach, leak, or loss as well as operational disruption.			
Management Action 1	Management will continue to complete the installation of windows across all applicable devices.	**Responsible Owner:**	**Date:**	**Priority:**
		Clair Stevenson	29/07/2022	**Medium**

Risk: Risk reference: 8004					Assessment:
Control	**Partial missing control** A Vulnerability and Patch Management Policy is in place., however, it does not include information such as testing requirements, roles and responsibilities, and the deployment process.				**Assessment:** **Design** × **Compliance** -
Findings / Implications	The patch and vulnerability management process was evidenced by way of change requests for the deployment of upgrades to test servers, configuration for the deployment of updates, the number of critical vulnerabilities, and third-party patch management amongst others. The Vulnerability and Patch Management Policy is documented as part of the ICT Security Management Policy. The areas of this policy that related to vulnerability and patch management outlined the timescales for applying patches/remediating vulnerabilities according to their criticality (critical and high within one month, medium and low within three months). In terms of vulnerability management, the policy further outlined the requirement for an IT health check to be completed annually as well as all infrastructure to be checked monthly for vulnerabilities. We received a previous IT health check document as well as a monthly vulnerability report. However, there was no other information clarifying the patch and vulnerability management process and strategy such as testing requirements (for remediation), roles and responsibilities, and the deployment process. Furthermore, on review of the script run to patch servers, the description provided at the header contradicted the statements regarding the timelines of patch deployment in that that the first week after patch, Tuesday is reserved for testing, the second week for downloading the updates to servers, then the third and fourth for applying the updates. When discussed with management, we confirmed that the wording in the script did not reflect current practices and needed to be updated. Without a more expansive vulnerability and patch management policy in place, there is a risk of mismanagement of vulnerabilities and patches as the direction and strategy is not clear and cannot be referenced by staff. This could result in an increased number of vulnerabilities in the estate which, if exploited, could result in a data breach, leak, or loss as well as operational disruption.				
Management Action 2	Management will expand the current Patch Management Policy to provide more information on the standards expected in areas such as: • Testing requirements; • Roles and responsibilities; and • Deployment process. Management will also update the script wording to ensure it reflects current practice.	**Responsible Owner:** Clair Stevenson	**Date:** 30/09/2022	**Priority:** **Medium**	

Risk: Risk reference: 8004				
Control	Patches are tested on lower priority servers before being deployed to higher priority servers. (However please note that there were servers in the IT Estate requiring updates).	**Assessment:**		
			Design	✓
			Compliance	×
Findings / Implications	The number of critical updates required across the server estate was provided which showed four updates were required. Of these four updates, the average installation was at 92 per cent. Evidence was also provided showing the patch management of servers through updates of replication test servers, change requests, and email communications sent out to the wider team notifying them of pending changes. Of the critical updates, there were 100 updates (25 per cent) labelled as “updates with no status” which could contain critical updates yet to be deployed. As part of the patching process, the patching team investigate these patches and manually patch the systems that have not reported a status although some patches may not be required by that system. A screenshot showing a breakdown of the current server patching levels of different groups (Priority 1, Priority 2 etc.) was received, and, on review, there were 86 Priority 1 servers that were labelled as “needing updates” which equated to 33 per cent of the server estate. If there are servers operating in the IT estate with vulnerabilities, there is a risk that these vulnerabilities are exploited which could lead to a data breach, leak, or loss as well as operational disruption.			
Management Action 3	Management will perform an assessment and apply all non-critical patches (where relevant). Management will investigate the “updates with no status” and apply any critical patches. Management will introduce governance practices to ensure there are no critical patches within the “updates with no status” e.g. through regular reporting.	**Responsible Owner:** Clair Stevenson	**Date:** 30/09/2022	**Priority:** **Medium**

Risk: Risk reference: 8004				
Control	Vulnerability scanning is in place to identify vulnerabilities along with remediation processes and reporting is made to the leadership team with any exceptions.		**Assessment:**	
			Design	✓
			Compliance	×
Findings / Implications	A Vulnerability Management Report was evidenced providing an overview for management and the leadership team of the current vulnerability status of the Force's estate. However, on review of the report from November 2021, 12 per cent of the estate had critical vulnerabilities and whilst this was a reduction from 86 per cent since October 2021 as noted in the report, with critical vulnerabilities existing in the estate, there is a risk that the vulnerabilities are exploited which could lead to a data breach, leak, or loss as well as operational disruption. Management could not provide an updated report as the latest vulnerability scan was not due until 31 January 2022 and throughout November and December 2021 the IT health check was being performed in conjunction with a change freeze.			
Management Action 5	Management will continue to remediate the critical vulnerabilities identified as a matter of urgency.	**Responsible Owner:** Clair Stevenson	**Date:** 01/07/2022	**Priority:** Medium

Risk: Risk reference: 8004				
Control	**Missing control** An intrusion detection system is in place, however, it was not being utilised.		**Assessment:**	
			Design	×
			Compliance	-
Findings / Implications	Intrusion detection capability within the organisation is in place through Microsoft 365 Defender. A screenshot was received of the dashboard which provided information such as devices and users at risk. However, on discussion with management we confirmed that whilst this capability is in place, it is not currently being utilised by the team. The justification for this being that the implementation of Microsoft 365 was completed during 2021 and other priorities were focussed on such as intrusion prevention. There is a plan to fully utilise the intrusion detection capability throughout 2022. Despite having intrusion prevention capability as well as monitoring and alerting processes in place, if intrusion detection is not fully utilised, there is a risk that potential security events are not identified which could lead to a data breach, leak, or loss as well as operational disruption.			
Management Action 6	Management will utilise the intrusion detection capability.	**Responsible Owner:** Clair Stevenson	**Date:** 30/09/2022	**Priority:** Medium

Risk: Risk reference: 8004				
Control	**Partially Missing Control** An Incident Management Policy is in place.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	The Incident Management Policy included the information that would generally be expected such as the remit of the process and any ties into other processes such as change and problem management. However, the document was dated 15 June 2020 and so has not been reviewed since that date. We have received evidence of the policy being complied with e.g. priority one incidents having post incident reviews and identifying root causes, However, without regular reviews of the policy, there is a risk that the current approved working practices are not followed which, in this case, could lead to the mismanagement of incidents which could lead to data breach, leak, or loss as well as operational disruption.			
Management Action 7	Management will review and update the Incident Management Policy. The policy will be reviewed on at least an annual basis going forward, or in the event of significant changes and/or incident learnings.	**Responsible Owner:** Clair Stevenson	**Date:** 01/08/2022	**Priority:** **Low**

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Risk	Control design not effective*	Non Compliance with controls	Agreed actions		
			Low	Medium	High
Risk reference: 8004	3 (15)	3 (15)	1	5	0
Total			1	5	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The internal audit assignment has been scoped to provide assurance on how the Chief Constable of North Yorkshire Police manage the following risk.

Objective of the review	Risk relevant to the scope of the review	Risk source
To provide assurance that computer systems and data are resilient to threats resulting from connection to the Internet.	**Risk reference: 8004**	Strategic Risk Register

The following areas will be considered as part of the review:

Secure Configuration

An assessment of the controls and process in place over the:

- Testing and installation of:
  - Security and critical patches applied to server infrastructure;
  - Patching of user endpoints;
  - Patching of third-party applications; and
  - Emergency patching.

Vulnerability Management

An assessment of the controls and process in place over:

- The vulnerability management policy.
- How the Force identifies vulnerabilities on the network (e.g. vulnerability scans, penetration testing).
- Remediation plans in place to resolve vulnerabilities.
- Reporting of management information on vulnerabilities.

Incident Management

An assessment of the high-level controls focussing on:

- Detection and triage of security breaches or unauthorised access attempts.

- Incident management and reporting process, including lessons learned.
- Reporting of management information on security incidents and their resolution.

Monitoring

An assessment of the tools and processes in place for:

- The continuous monitoring of security events across the network.
- The continuous monitoring for anomalous behaviour (e.g. risky logins, personal data download, etc.).
- Intrusion detection and prevention system(s).
- The alerting and triage procedures in place to detect and report security incidents.

The following limitations apply to the scope of our work:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of cyber security risk.
- The approach taken for this review will be to validate the design of controls and testing of key controls.
- We will be testing key controls on a sample basis and for the financial year 2021/22 only.
- We will not perform penetration tests and vulnerability assessments however we will review the results of tests undertaken by independent service providers.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the cyber security environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting cyber security and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	7 February 2022
Draft report issued	23 February 2022
Revised draft report issued	11 May 2022
Responses received	30 May 2022
Final report issued	30 May 2022

Internal audit Contacts	Daniel Harris, Head of Internal Audit
	Philip Church, Senior Manager
	Mike Gibson, Manager
	Paul O'Leary, Technology Risk Assurance (TRA) Partner
	Rich Dillon, TRA Associate Director
	Louis McGrath, TRA Senior Consultant
Client sponsor	Gordon McQueen, Head of ICT
Distribution	Gordon McQueen, Head of ICT Clair Stevenson, Service Delivery Manager

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Chief Constable of North Yorkshire**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.