

**Audit and Risk Assurance Committee (ARAC)**

**Cyber Security Quarterly Update**



**Audit and Risk Assurance Committee (ARAC)**

**Date:** 8 June 2023 **Paper reference:** AUD 22/23 **Agenda item:** 8

**Author:** Louise Dineley

**Protective marking:** OFFICIAL

### Cyber Security Quarterly Update Purpose of paper

The Cyber Security dashboard provides a summary of cyber security systems and protection and builds on the detailed report provided to ARAC in January 2023. It covers the period January – May 2023.

### Decision making to date

1. The Cyber Security Quarterly Update is presented for the committee to note.

### Action required

1. ARAC Members are required to note the Update.



**ARAC Cyber Security dashboard**

Update June 2023 AUD 31/22

## Introduction



The Cyber Security dashboard provides a summary of cyber security systems and protection. The high level summary builds on the detailed report provided to ARAC in January 2023 and cover the period January – May 2023.

The HTA’s approach to the strategic management of cyber security risks and threats is based around 6 key outcomes. Our approach aims to implement measures to achieve the mandatory protective security outcomes of the Minimum Cyber Security Standard. The HTA’s cyber security systems are focused on the following outcomes:

**Identify :** We have in place appropriate cyber security governance processes. We have identified and catalogued the sensitive information we hold. We have identified and catalogued the key operational services we provide. The need for users to access sensitive information or key operational services is understood and continually managed.

**Protect :** Access to sensitive information and key operational services is only provided to identified, authenticated and authorised users or systems. Systems that handle sensitive information or key operational services are protected from exploitation of known vulnerabilities. Highly privileged accounts are not vulnerable to common cyber-attacks.

**Detect :** We take steps to detect common cyber-attacks.

**Respond** : We have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.

**Recover :** We have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.

## Cyber security Performance – at a glance (January – May 2023)



93.26%

Microsoft secure score

48

Viruses intercepted Since January 2023

0

Device exploit availability (no known)

A total of 0 devices had 15 known vulnerabilities

Device vulnerability

Total requests: 225840 Number of blocks 4784

Internet use: Identified access

4

(1 relevant to HTA)

RTANCA Alerts received from NHS X

100%

Number of RTANCA alerts responded to in 48hrs

100%

Staff mandatory training (Completed 2023)

New accounts 8

Disabled accounts 6

Staff accounts Jan-May 2023

Identified 69 user accounts

4 admin accounts All set up to authentic

via MFA

User account Audit May 2023

**ARAC Cyber Security Dashboard – Overview**



The dashboard below provides an overview of our systems and the level of risk depicted by a RAG rating. This is data that is automatically generated through our systems, interpreted and accessed through the NHS Threat Protection portal. This presentation provides assurance that HTA ‘s protection systems are performing as intended.

|  |  |  |
| --- | --- | --- |
| Microsoft Secure Score | Antivirus Update Status | HTA Exposure Score |
| 93.26% |  |  |
| similar NHS entities | 100% out of 120 |  |
| scored 45.48% | devices |  |
| Meaning we have well | MS Defender identifies | 35% |
| defined and managed | devices as laptops and |  |
| processes in place | servers |  |

48 Viruses over 5 months 0.1% of mail received

60 Phishing attempts sent to 26 recipients.

Phishing & Viruses Detected

|  |  |
| --- | --- |
| Spam Detected | |
| Month | Count |
| Jan | 539 |
| Feb | 575 |
| Mar | 724 |
| April | 725 |
| Total | 2563 |

Secure score is a defined standard that shows how well we are protected. It also shows how we compare to similar NHS entities.

This shows we are significantly better

Our Antivirus solution is monitored and updated real time ensuring we have the latest known virus threat and unknown breaches kept to a minimum

Higher the score the more at risk our devices are 35% is in the medium bracket.

This increase is due to disposal of old laptops still waiting to be removed from ATP but are all currently stored with our IT

The high proportion of remote working means that email viruses and phishing attempts have never been more prevalent. The HTA identified 48 viruses included in email, all of which were intercepted by our security systems.

SPAM accounts for 11.7% of all inbound email. This figure is what was intercepted by our security systems. User feedback is critical in the event that spam breaches these controls.

Incidents are reported to IT for follow up.

# ARAC Cyber Security Dashboard IDENTIFICATION & PROTECTION Summary



**4784** requests to access to sites flagged as representing potential risk categories. Further follow up has not identified any concerns although has identified “social media” sites as a recurring theme.

Web Monitoring & Filtering

The HTA has well defined Advanced Threat Protection systems in place as a result of taking advantage of the NHS arrangement. As part of these systems we are part of an alert system and are required to Respond to NHS Cyber Alerts (RTANCA). These are underpinned by a comprehensive set of policies and procedures that allows the monitoring and governance of all sensitive data and requests from GDPR to FOI and access to confidential/personal information internally. This dashboard is an indicator of the policies and controls we have in place to address and manage request and incidents that directly relate to information potentially being extracted for malicious purposes.

58 devices with no known exploit is considered good. Devices in this context includes Servers Routers and other Infrastructure devices.

An exploit is an attack that leverages a known vulnerability. Even though there are vulnerabilities identified they may not be exploitable as they have further security controls to prevent the attack

**0** Exploits Verified 1 Critical

**0** Exploits Available 6 High

**58** No Known Exploit 0 Low

Device Exploit Availability & Device Vulnerability Severity

0% of Machines affected 0% Blocked due to gaming

Greater than 50% Social Media/Streaming/Web Mail

WWW Analysis

# ARAC Cyber Security Dashboard DETECTION Summary



In addition to existing systems and services, vulnerability may also be introduced by new or replacement systems. The risk of fraud is one specific vulnerability assessed as part of any new digital development.

As at April 2023 no new digital systems had been introduced requiring a Fraud Risk Assessment

Other potential vulnerabilities

ASR polices are critical in the protection of mitigating misuse of equipment and preventing cyber threats. Currently applied to all active devices

Attack Surface Reduction

|  |  |
| --- | --- |
| Potentially malicious events | Health State/Patch management |
| ATP identified the following security attacks and successfully remediated the issues  1 Detections  0 Unique Files  1 Affected Devices |
| ATP identified 54 Active devices in the HTA estate and automatically applies security policies and default usage policies such as not allowing the use of unauthorised external USB devices  Patches to active devices are 100%complete  63 Inactive devices are currently being held by IT waiting disposal and will account for any health variances. |
| Exposure Distribution |
| Of the malicious threats  **0 device was at high risk devices medium**  **50 devices low**  To note the same device can be in all 3 categories depending on the type of risk. This was not a factor for this period | Website Vulnerabilities |
| Following the redevelopment of the website the HTA monitors potential vulnerabilities on its public facing website.  As at April 2023 no vulnerabilities had been identified on the independently generated monthly reports. |

**ARAC Cyber Security dashboard RESPONSE & RECOVERY Summary**

NHS Cyber Security Alerts

There are a number of different routes through which the HTA can be alerted to potential malicious activity. Not all notifications need to be formal alerts or actual incidents. Events may also include near misses where control systems have prevent access. Notifications can come from different sources including are own system monitoring, reported incidents, monitoring by the Cyber Security Unit and RTANCA alerts. NHSx & NHS Digital require the HTA to respond to critical alerts within 48 Hours. Not all are applicable to the HTA but we have met all the required responses for those that affected us. In addition notifications of potential malicious activities identified through external monitoring have already been identified internally.

Top Vulnerable Software

Windows Server Windows 10 Google Chrome Microsoft Edge

IT are making recommendations to remedy.

Backup recovery

We have tested periodically via requests from staff to recover files from servers. We are planning a server backup recovery in tandem with our CIRP

Backups to our production servers are completed daily with our Finance servers being backed up hourly

Our offsite DR live servers are backed up weekly

Backup Jobs schedule

|  |  |  |
| --- | --- | --- |
| NHS Cyber Security Alerts | HTA Affected | RTANCA  Responded to within 48 Hours  100% |
| Total of 4 alerts 4 High  1 Medium  0 Low | 4 request were made 3 were not applicable  1 were addressed and dealt with |
| Internal Monitoring security incidents | | |
| Since January 2023 there have been 49 failed log on attempts. These incidents are near misses as although there has been an attempt to log on externally, controls within the system identified an unusual sequence in the log on attempts and these were blocked. | | |



# IT Risks



Risk 7 of the Strategic Risk Register identifies a specific risk.

*SRR 7: Failure to optimise the safe use of existing and emerging digital data and technology*

This is further broken down through the IT operational risk register which identifies the following risks. These risks are all subject to management controls.

* IT service disruption
* Cyber security threats
* Data breach
* Service delivery failures
* Mobile device management

# ARAC Cyber Security dashboard Staff Awareness Training

Cyber Security Training Completed

Mandatory Cyber Security Training

Planned Realtime Simulated Security Training



Information Security Training

Q4 2022/23

Personal Data Security Physical Risks – Information Security

Toolbox (talk) Consequences of Cybercrime

These tests are part of the NHS ATP security toolkit to test all HTA staff in:

* Malware Attack
* Phishing Attempts
* Credential Harvest (attempt to obtain personal information)
* Link to Malware Attack
* Consent Grant Attack (this is when you give access to data that do not have the right to see it)

The reports will identify those who pass or fail so more detailed training can be given. The tests are currently being scheduled.

## Conclusion



* Over the last quarter the HTA’s cyber security threat protection has been maintained via existing monitoring systems and responding to regular alerts via the RTANCA (Response to an NHS Cyber Alert) system.
* All issues identified either through detection, reports or alerts have been actioned without risk to the organisation.
* The information highlights the HTA is in a good position to monitor and protect its systems, devices and users from potential attacks.
* The continual threat and creativity of cyber attacks means that in addition to maintenance of existing systems we need to continue to seek opportunities to improve the security of IT systems and digital data stores.

# Annex A: Security Incident Management

The following flow chart summarises the HTA’s process of identifying and managing potential vulnerabilities within the HTA’s systems including remedial action, assurance and securing additional expertise as necessary.

Security incident / alert received by HTA



(note multiple sources including RTANCA, NHS Cyber alerts etc))

Assessment of relevance to the HTA

Risk assessment and determine action required including timing

Internal monitoring via HTA systems (BCC)

Investigation as required to determine root cause, vulnerabilities or effectiveness of controls

Investigation and remedial action (includes learning from near missed)

Additional investigation expertise may need to be accessed (note NHS contracts

CFMA)

Assurance



(Reports to Director of DTD, SIRO & ARAC)

External reporting and assurance if and as indicated