# JULY UNIT REPORTS

HEALTH SCIENCES
CHIEF INFORMATION OFFICE

***APPLICATIONS - RAY AVILA***

***SYSTEMS - PHIL MARQUEZ***

***SECURITY - MIKE MEYER***

***TECHNOLOGY SUPPORT - RICK ADCOCK***

***FOR MORE DETAILS:***

**Marcia Sletten**, msletten@salud.unm.edu

# APPLICATIONS TEAM

## ACCOMPLISHMENTS

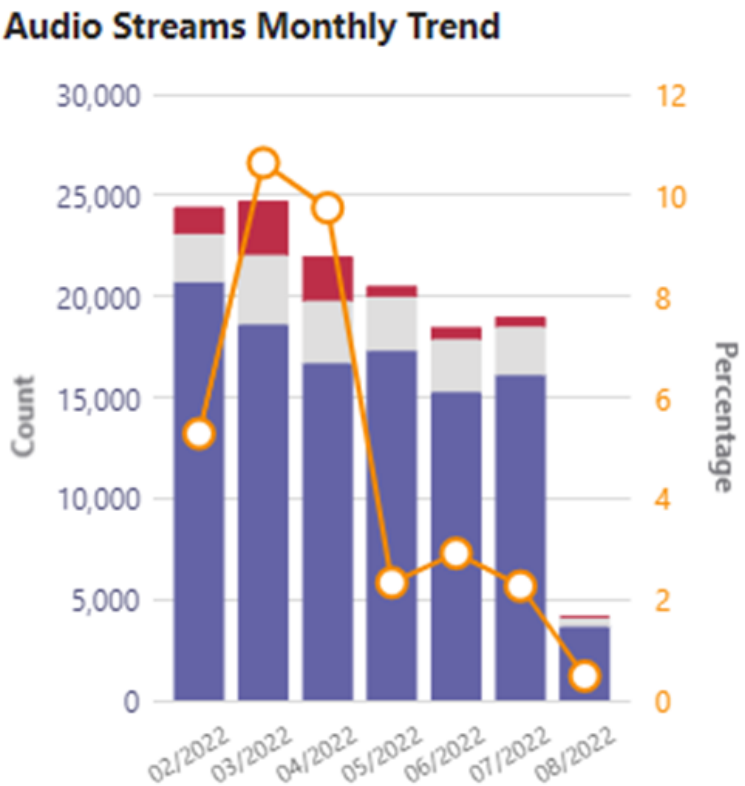
- Decommissioned legacy SharePoint 2010 servers
- Completed a number of fiscal year processes
- Created MD 2026 class in OMSA database

## IN-PROGRESS

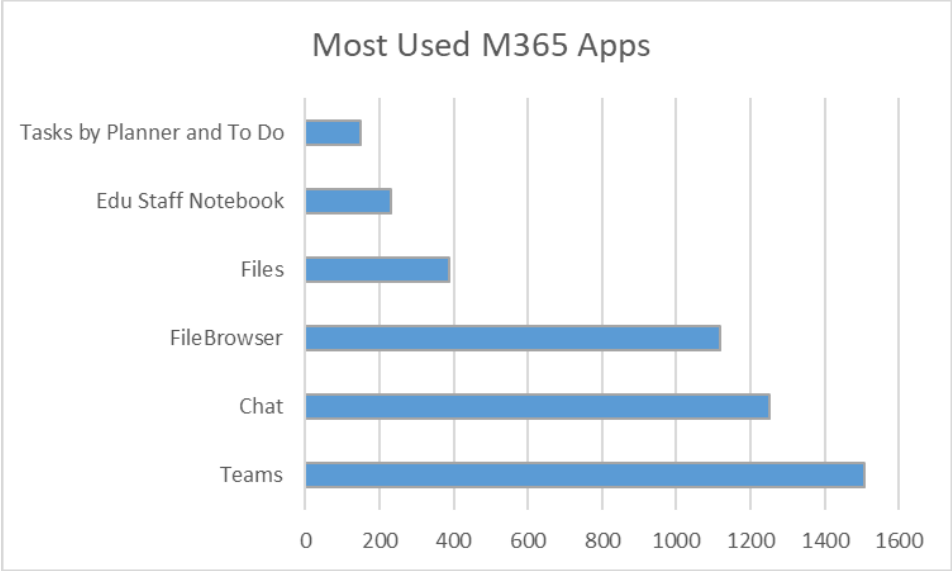
- Zoom Security Enhancement
- M365 Intune Implementation

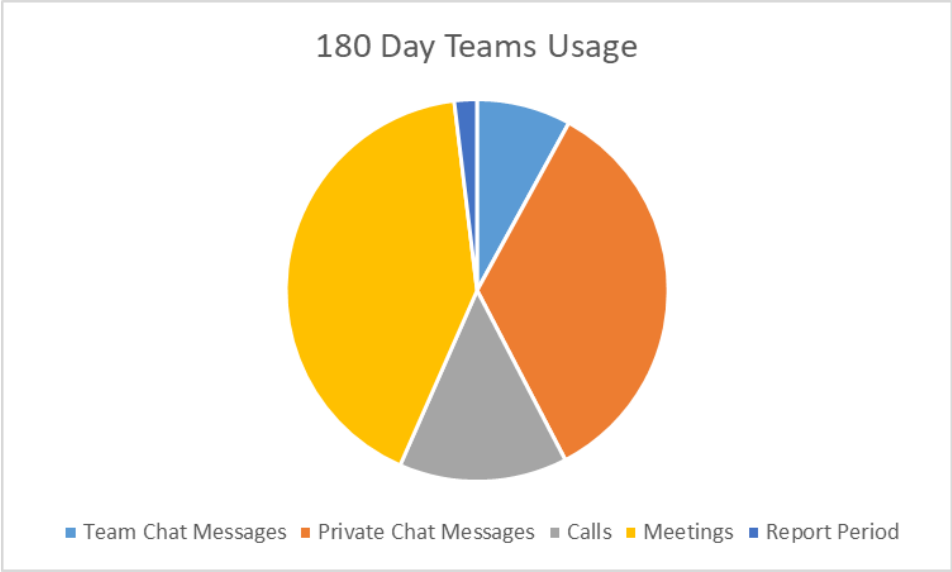
## METRICS

- M365 Teams Call Quality Improvement:



# METRICS *(CONTINUED)*



# SYSTEMS TEAM

## ACCOMPLISHMENTS

- No new major projects in June
- On Site Network Attached Storage replacement (Pure Storage)
  - Final migrations of network folders from NetApp (H:\Home) to new Pure Storage appliance still pending.  Will complete in next maintenance window
- Completed July monthly HSC Systems maintenance window on May 21 (7-9am)
  - Passwordstate Update
  - Extend hsc-iechoprod2 drive
- Posted backfill position for Systems/Network Analyst 3
  - Scheduled interviews for SNA3
- Metallic cloud backup
  - Completed move of primary backup storage from Metallic Hot tier to Cool tier to reduce costs
  - Removed duplications, modified retention plans to reduce overall storage requirements to within the estimated 250TB to manage 165 FET (front end terabytes) of covered data

## IN-PROGRESS

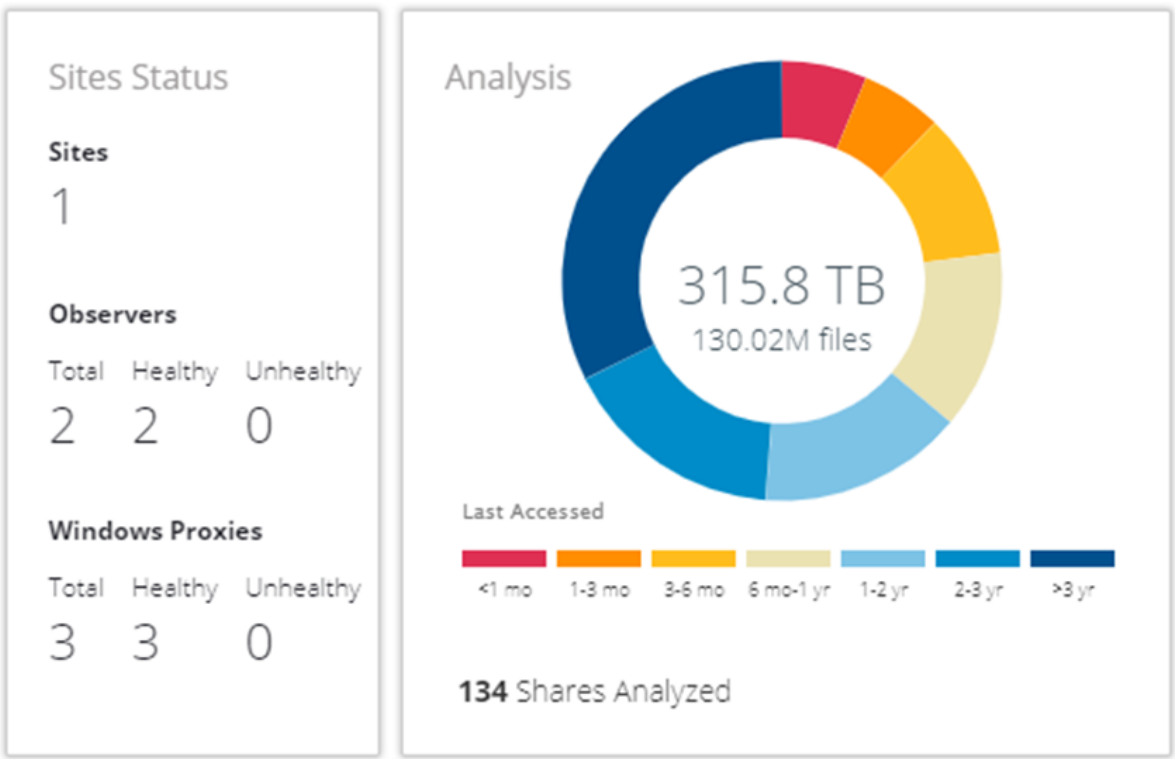
- Metallic cloud backup
  - Still working to add licensing to provide Metallic backup for remaining unprotected data.  All data on NetApp filers was retained with shadow copies, versioning, and replication.  This will extend cloud backup and ransomware protection to include that data as well.
- Planning for August Monthly maintenance period – 7/16/22 from 7-9am
  - Complete final \Home directory cutovers
  - PACS server reboot
  - Hyper-V migrations to Nutanix

## IN-PROGRESS *(CONTINUED)*

- New Hyper-V h/w for HA cluster being delivered.  Install planning for September install
  - Pending delivery of Shared Storage Array
- Identifying shared services between HSC, UNMH, and UNM systems teams.
  - Initial meetings planned for early August

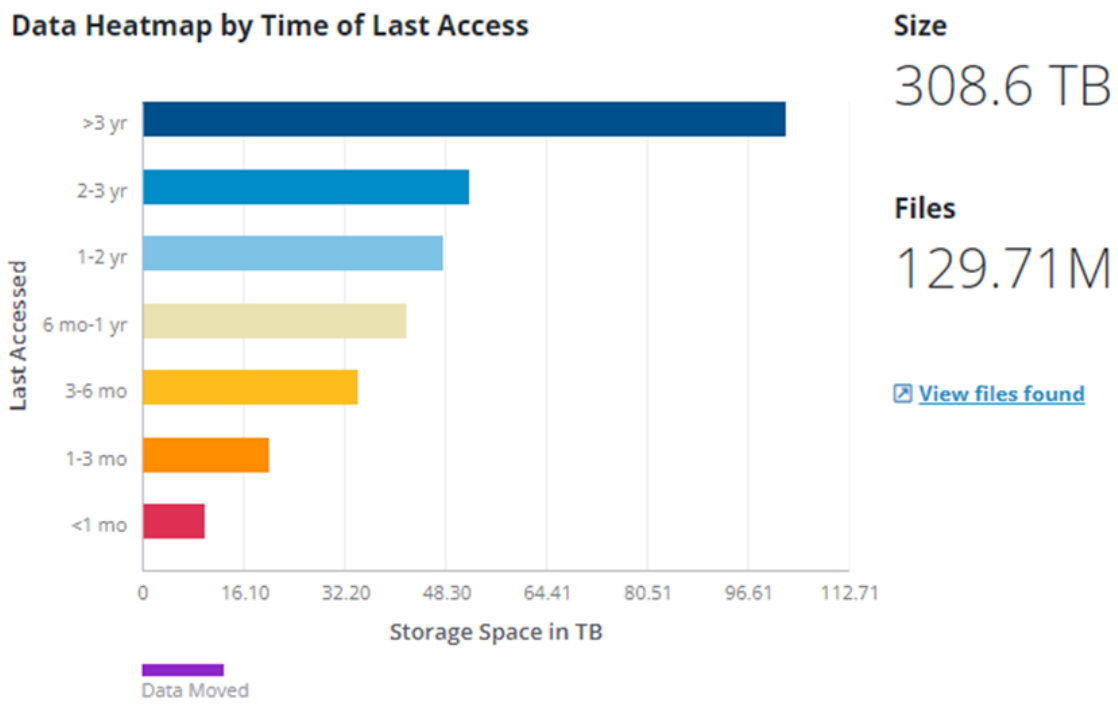
## METRICS

- System availability
  - No systems downtime
- This month's updates from Komprise Data Analysis tools showing graphs and metrics across all data stores
  - Aging reports showing data volumes by Last Accessed Dates
  - Capacity projections
  - Space consumed by Top Shares



# METRICS *(CONTINUED)*

| 201.7 TB | 58.9 TB/yr | 211.7 TB |
|---|---|---|
| Inactive over 1 year | Data growth rate over 1 year | Capacity needed in 3 years |




# RECOGNITION

- Bob Gagnon for covering while much of the team was out of office.

SYSTEMS TEAM

# INFORMATION SECURITY OFFICE

## *ACCOMPLISHMENTS*

| ACCOMPLISHMENT | IMPACT |
|---|---|
| Provided the CIO with various options for re-organizing the three separate cyber security departments – ISO, Network Security and Cybersecurity. | More efficient cyber programmatics and operations will result. |
| Investigated two disclosures of student data at the request of the HSC Registrar. | Minimize risk due to unauthorized disclosure of FERPA information |
| Network Security and ISO ran two phishing "challenges" in July. | Reducing successful phishing attempts reduces our risk exposure to ransomware attacks. |
| Initiated a "Cyber Security Processes and Forms" JNIS sub-team. | This sub-team is chartered to develop sound processes and forms pertaining to risk assessment and including vendor risk assessments. The goal is a consistent risk assessment process across the enterprise. |
| Participated in various planning meetings for upcoming CLA assessment, which begins 22 August. | CLA audit will encompass the entire network this year, not only clinical functions. |

# *IN-PROGRESS*

| ACTIVITY | OBJECTIVE(S) |
|---|---|
| Improve Cyber Security Incident Response | Bring clarity to our incident response policy and plans. Provide "ransomware playbook" to speed response in the next incident. Conduct a major incident response in October 2022. |
| Improve Interior Security Controls | Implement additional security measures to limit lateral movement on our network if another attack penetrates our perimeter defenses. |
| Phishing Training | Conduct effective training in recognizing phishing attacks. Our target "click rate" is 5%. Current rate is 20-30%. |
| Vulnerability Management | The goal of this effort for 2022 is to identify and begin to reduce our critical vulnerabilities. We have completed the first phase of this effort by successfully deploying a new product (Tenable.IO) to scan the entire network. Now the work is remediating the vulnerabilities found. |
| Protected DNS (pDNS) Collaboration with Main Campus | pDNS relies on threat intelligence to filter suspicious Internet addresses and is one of the major defenses against phishing, therefore ransomware. Collaboration with Main Campus will reduce overall cost for the service. |
| Risk assessment process improvement. | Improve cyber security risk assessment consistently across the enterprise. |

# METRICS

| | |
|---|---|
| Change requests | 7 (1 emergency request) |
| Certificate requests | 2 |
| Software and Cloud service security reviews | 24 |
| DUA/SFTP Data Transfer Support Requests | 17 |
| Other Support Request | 36 |
| Perimeter Vulnerabilities | Critical – 0<br>High – 1<br>Medium - 39<br>Low - 16 |
| Root Cause Analysis submissions | 0 |
| Critical Vulnerabilities on servers | JUL – 1444 total; 81 unique; 606 systems |
| Malicious email blocked by email firewall | 16,905,925 |
| Outbound email blocks for PHI content | 144 |

Perimeter Vulnerabilities
JUN 2022


Perimeter Vulnerabilities
JUNI2022

## METRICS *(CONTINUED)*

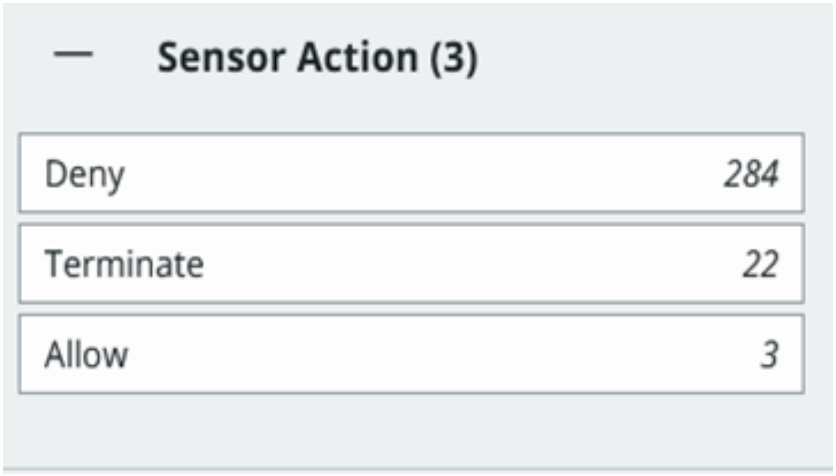
Proofpoint Messages Processed and Rejected June 2022

| Type | Messages | Percent |
|---|---|---|
| Blocked:PDR | 14449529 | 64.88% |
| Accepted | 5365226 | 24.09% |
| Blocked:Email Firewall | 1719750 | 7.72% |
| Blocked:Spam | 409340 | 1.83% |
| Blocked:Others | 326708 | 1.46% |
| Blocked:Regulatory Compliance | 298 | 0% |
| Blocked:Anti-Virus | 204 | 0% |
| Blocked:Zero-Hour | 96 | 0% |
| Total | 22271151 | 100% |

Notes: PDR = Proofpoint Dynamic Reputation service

"Regulatory Compliance" = Outbound email containing ePHI not properly encrypted

Carbon Black Endpoint Detection and Response - Threats Denied July 2022




## RECOGNITION

- I want to express my appreciation for Roy's service to this team. I know he generated some chaos, but he generated some long-needed change. As we say in the Navy, "Fair winds and following seas, Roy."

# TECHNOLOGY SUPPORT

## ACCOMPLISHMENTS

- Enabled auto provisioning for SailPoint Entitlements
- Developed a UNM SSL Cert/Cert Trust Library
- Completed creating a workflow for requests to unblock Multi-Factor Authentication lockouts
- Upgraded Tomcat on all identity management servers to address vulnerability

## IN-PROGRESS

- Testing softphones for off-site access to the Automated Call Distribution system
- Continue Microsoft Intune implementation
- SailPoint 8.3 upgrade
- Working on Intune enrollment for Mac devices
- Mac Operating System Beta Testing
- Early development of Device IQ (managing devices) similar to IdentityIQ (managing identities)
- Changing the deployment of student workstations in the library

# METRICS

## HSC IT Tier 2 Key Performance Indicators (Workstation and Classroom Groups)

### January 2022 -June 2022

| Ticket Volume Workstation Group | | | | | | | |
|---|---|---|---|---|---|---|---|
| | January | February | March | April | May | June | Total |
| Incidents | 25 | 3 | 21 | 18 | 13 | 9 | 89 |
| Service Requests | 202 | 162 | 171 | 158 | 199 | 198 | 1090 |
| Total | 227 | 165 | 192 | 176 | 212 | 207 | 1179 |
| FTE | 3 | 3 | 2.5 | 2.75 | 3 | 2.75 | |

| Key Period Projects: |
|---|
| Release Windows Gold Image |
| Clean up VPN access between HSC and UNMH |
| SAML Proxy for application access with main campus |
| Implement NOMAD for Mac binding to Active Directory |
| Implement the workstation hardening group policy |
| On-Board HSC Web Team in Cherwell |
| Remediation of unencrypted devices |
| Completed changes to the Azure multi-tenant synchronization |
| Created a new monitoring station for service monitoring |
| Finished AV deployments for the Center of Orthopedic Excellence |
| Expired passwords for all account that were not registered for MFA |
| Backfill Carbon Black for older OSX devices that could not be done automated |
| Configure Microsoft Intune for enrollment, windows patching, and compliance reporting |
| Testing softphones for off-site access to the ACD |
| Created pass phrases to replace current password methodology |
| Remediate Windows 7 workstations |
| Testing Microsoft Intune for workstation management |
| Working with UNMH on the deployment of Dragon Medical One |

# METRICS *(CONTINUED)*

| Ticket Volume Classroom | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | January | February | March | April | May | June | Total |
| Incidents | | 11 | 20 | 9 | 12 | 13 | 8 | 73 |
| Service Requests | | 9 | 3 | 6 | 2 | 7 | 3 | 30 |
| Total | | 20 | 23 | 15 | 14 | 20 | 11 | 103 |
| FTE | | 4 | 3.5 | 3.5 | 3.75 | 2.75 | 1.5 | |

**Key Period Projects and Information:**

- Seven classroom upgrades to this point
- Five classroom upgrades in progress
- Two upcoming construction projects ISUB and CON/COPH building includes:
  - 6 classrooms
  - 10 conference rooms
  - various study areas
  - digital signs
- GEER Grant Administration
- Digital Signage
  - 18 sub accounts
  - 49 displays (24 of them exclusively managed by CTU)