APRIL 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

- Recreated 20+ Legacy Exams in Learning Central
- Continued planning for HSC Canvas implementation
- Implemented Cyber Security Evaluation Tool (CSET) for HSC ISO
- Encrypted RECIST and CRTC databases
- Updated PA Supplemental Application
- Provided FY22 data to Faculty Retention project
- Updated yearly VA Salaries

IN-PROGRESS

- Zoom Security Enhancement
- M365 Intune implementation

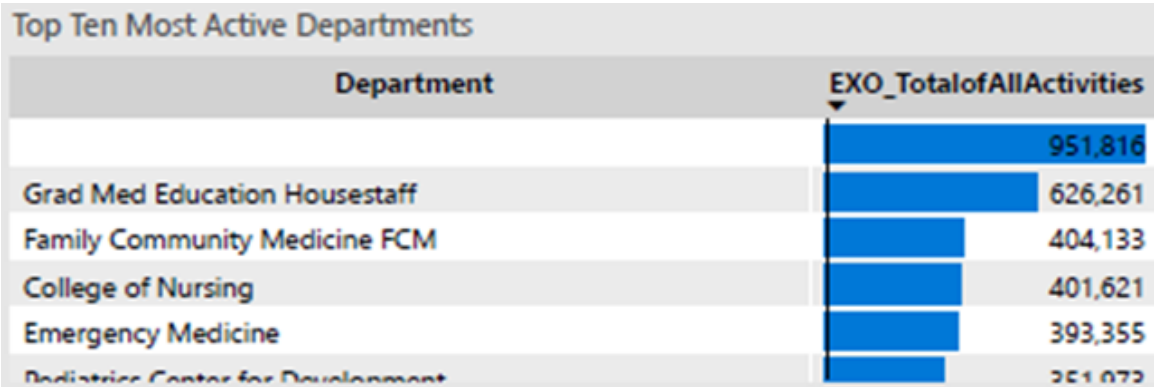
METRICS

- M365 Device Usage

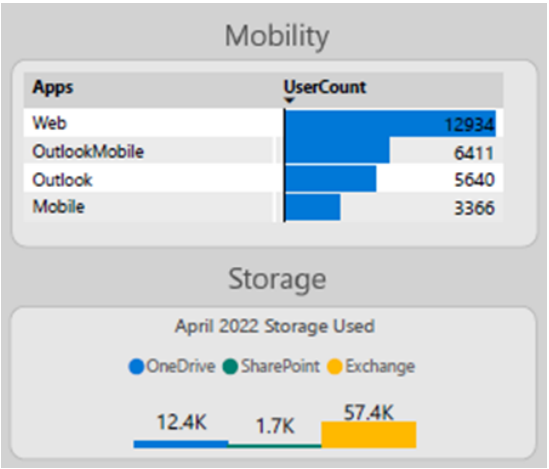
Year	Android Count	iOS Count	Mac Count	WinRt Count	Pc Count
2021					
June	602	840	652	3	1,694
July	662	971	740	4	1,881
August	779	1129	832	6	2,098
September	862	1265	906	8	2,251
October	958	1414	979	9	2,405
November	1015	1537	1057	9	2,536
December	1043	1608	1101	10	2,610
2022					
January	1087	1725	1164	13	2,749
February	1100	1784	1182	18	2,868
March	1144	1885	1231	19	3,032

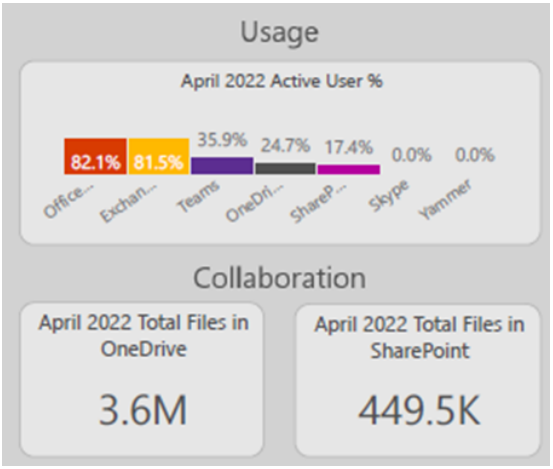
METRICS *(CONTINUED)*

- Department activity within M365



- Mobility and storage in M365





SYSTEMS TEAM

ACCOMPLISHMENTS

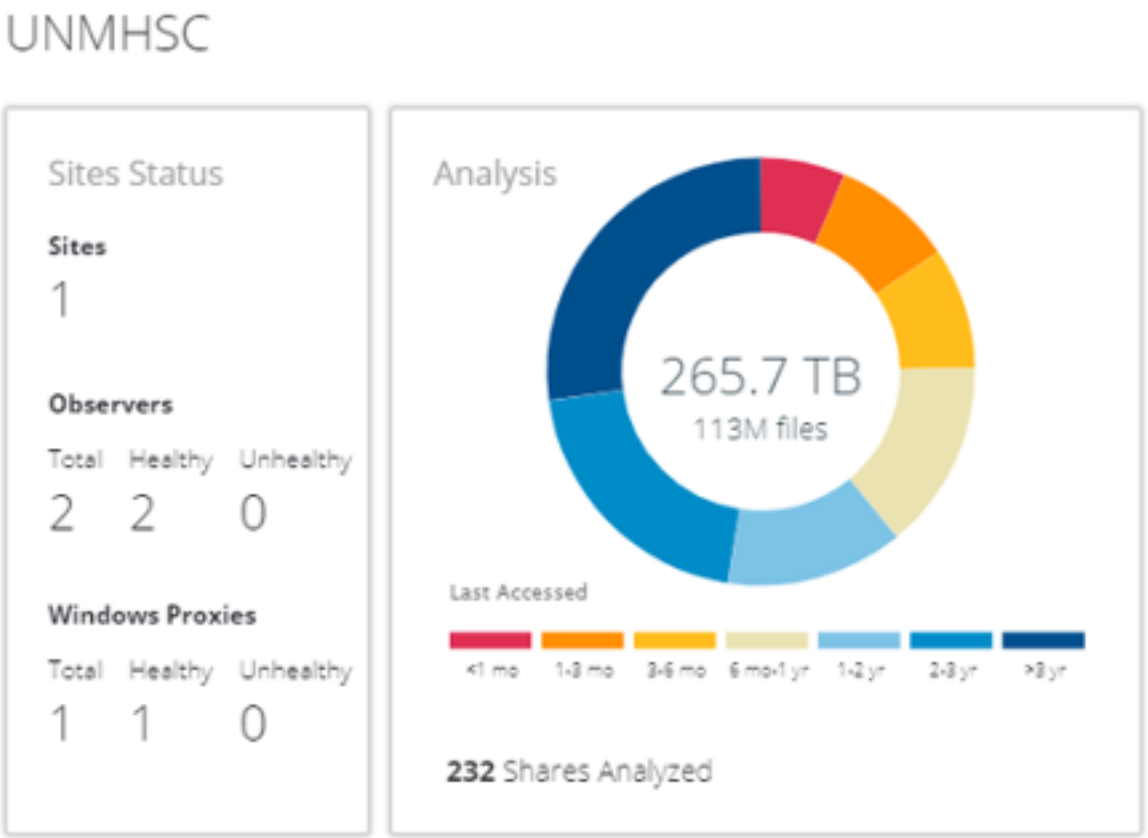
- No new major projects in March
- On Site Network Attached Storage replacement (Pure Storage)
  - Began migrations of network folders from NetApp and Dell NAS (H:\Home, O:\ and N:\)
  - Secured licensing through Pure Storage partner for Komprise migration/replication/data analytics tool to move existing data to new storage appliance, replicate to secondary storage and provide deep analytics of data and storage utilization
- Completed investigation of redundant cooling options for BRF data center
  - The current HVAC system is a single point of failure for the data center
  - 2nd Liebert chilled water system will cost ~75k to purchase and install through UNM FM
- Received Change Board approval for monthly HSC Systems maintenance window.
  - Will occur 7-9am on the third Saturday of each month starting May 21.
  - Communicated to leadership teams and through HSC Communications with FYI to UNMH Oversight Committee.

IN-PROGRESS

- Attending NIH STRIDES Initiative sessions to simulate a research scenario
  - Excellent hands on learning opportunities in building out storage and virtual server environment within Azure as part of STRIDES POC for research. Will be instrumental in future production implementations.
- Metallic cloud backup
  - Continued working with vendor on quotes to extend Metallic backup service to CDD servers and virtual machines
  - Finalizing details 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.

METRICS

- System availability:
  - No systems downtime
- Still working on completing standardized patching for domain controllers
  - Issues with SCCM being worked with Microsoft
- We now have full access to Komprise Data Analysis tools to provide graphs and metrics across all data stores
  - Aging reports showing data volumes by Last Accessed Dates
  - Ongoing Migrations
  - Space consumed by Top Shares

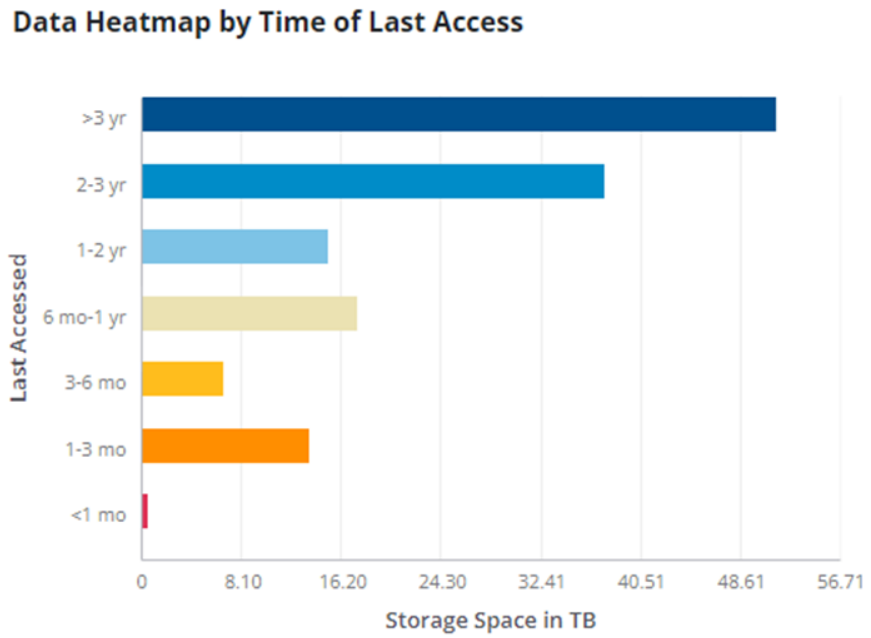


Migrations

Active	Paused	Actionable errors	Ready for cutover	Ready for final	Completed
27	0	8	0	2	31

Site	Active	Paused	Actionable errors	Ready for cutover	Ready for final	Completed
UNMHSC	27	0	8	0	2	31

METRICS *(CONTINUED)*



Size

142.5 TB

Files

90.43M

View files found

RECOGNITION

- Jason Barnes and Lin Ye for their efforts to assist in testing connectivity between cameras in HSC parking lots and UNM PD

INFORMATION SECURITY OFFICE

ACCOMPLISHMENTS

ACCOMPLISHMENT	IMPACT
Responded to extensive data call from the Office of Civil Rights (OCR) concerning our ransomware attack in Apr 2021.	We hope to proof to OCR that we had adequate security controls in place before the attack and have made substantial improvements following the attack.
Entire ISO team participated in Planet Technology training on using and securing Azure infrastructure as part of Innovation Center/STRIDES project.	May provide new AI and ML tools to improve tools available for HSC researchers.
ISO team participated with UH Network Security and UH Cyber Security in a threat hunting exercise sponsored by one of our vendors.	Threat hunting in the cyber world involves searching and understanding security logs. This was excellent training that will improve our team's ability to recognize threat activity and respond more quickly in the event of a future ransomware attack.
Tenable.io Vulnerability Scanner – Provided training and access for dept IT tech to review vulnerability reports for their assets.	Vulnerability management requires cooperation between the cyber security analysts who identify the vulnerabilities and IT techs who in most cases are needed to remediate them. Giving them access to the scanner allows the more proactive and security aware techs to be proactive.

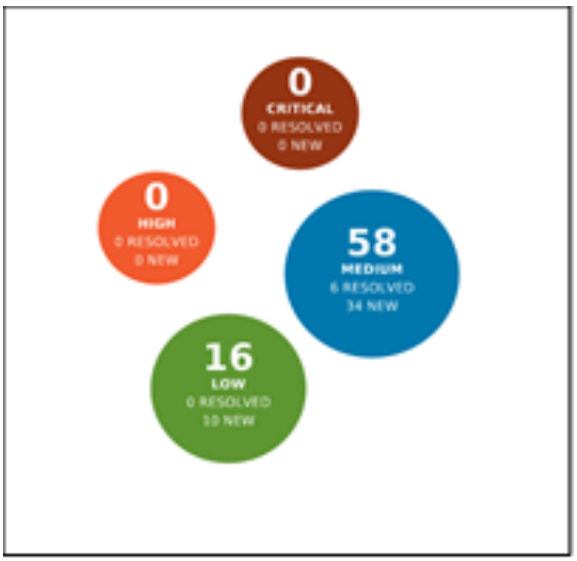
IN-PROGRESS

ACTIVITY	OBJECTIVE(S)
Implement Innovation Center Cyber Security using the U.S. government Cybersecurity Maturity Model Certification (CMMC) standards.	Conduct and document security reviews and establish security controls that are consistent and acceptable for the processing of ePHI in a cloud environment.
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 Oct 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 around 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.

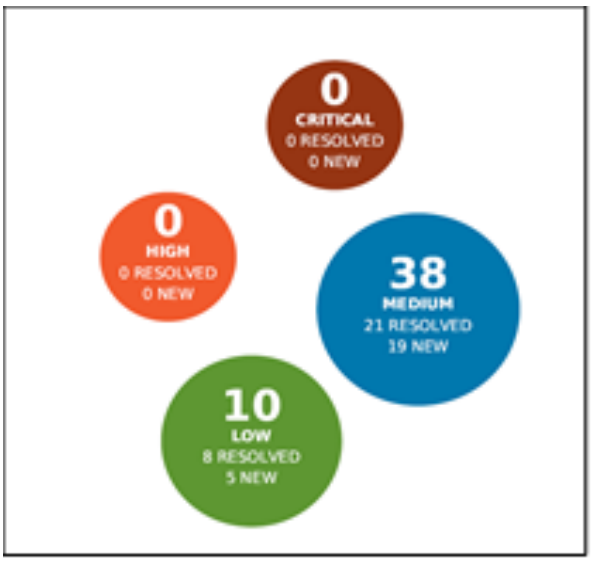
METRICS

Change requests	13
Certificate requests	3 new, 4 renewals
Root Cause Analysis submissions	3 closed
Software and Cloud service security reviews	20
DUA/SFTP Data Transfer Support Requests	28
Other Support Request	48
Vulnerability Scans	14
Perimeter Vulnerabilities	Critical – 0 High – 0 Medium - 38
Enterprise Critical Vulnerabilities (entire	34,642
Malicious email blocked by email firewall	28,846

Perimeter Vulnerabilities March 2022



Perimeter Vulnerabilities April 2022



Proofpoint Email Firewall

TECHNOLOGY SUPPORT

ACCOMPLISHMENTS

- Released the new series of Dell Latitude laptops
- AV upgrade of Domenici Center Room 3740
- Created new monitoring station for services in HSLIC room 317

IN-PROGRESS

- Remediation of unencrypted workstations
  - Departmental IT staff remediating their workstations
  - HSC IT staff remediating the remaining workstations (15 fixed, 18 more contacted)
- In-Tune configuration for enrollment and workstation management
  - Intune for OSX enrollment process in Apple School Manager, and management configuration
  - Windows Patching
  - Compliance Reporting
- Password Policy re-design for pass phrases
- Using NoMad for AD bind issue of OSX devices
- Testing Soft-phones for off-site access to the Automated Call Distribution system

METRICS

Remaining Windows 7 Workstations (other than those identified as being connected to equipment)

DEPARTMENT	COUNT
Administration	2
Center for HPV Prevention	3
FMC	1
Institute for Public Health	1
Internal Medicine	12
MGM	2
Neurology	3
Pathology	1
Pediatrics	1
Radiology	2
Tele-Health	1
UNMH	47