



**HEALTH  
SCIENCES**  
CHIEF INFORMATION  
OFFICE

## **APRIL UNIT REPORTS**

**APPLICATIONS-RAY AVILA**

**SYSTEMS-PHIL MARQUEZ**

**SECURITY-MIKE MEYER**

**TECHNOLOGY SUPPORT-RICK ADCOCK**

**UH IT NETWORK/NETSEC-CHARLIE WEAVER**

**HSC 2021 VISION**

# APPLICATIONS

RAY AVILA

## Accomplishments

- Assisted with launch of new cancer center web site
- Coordinated with vendor to set up publishing to eWay test hosting environment for unmhealth.org
- Identity IQ/Sailpoint training
- Provisioned 103 new Zoom Pro licenses
- Developed instructional materials for Radiology and SOM UME
- Conducted 5 Learning Central training sessions for new LC administrators
- Modifications to CITI Covid Back To Campus materials in LC
- Moodle instructional consultations
- Course administration activity for annual required training courses and various Moodle courses

## In-Progress

Projects in flight	Status
Sharepoint Online / m365 transition – Active	3/1/2022
Unmhealth.org vendor hosting	5/17/2021
Faculty Directory implementation	5/20/2021

## Metrics

- SP2010 EOL activity tracking:
  - Total sites: 73
  - Awaiting assessment - 70
  - Migration to SPO in process – 2
  - Migration to alternative platform in process – 1
  - Requiring vendor assistance: N/A
  - Marked for deletion/abandonment: N/A

\*Graphs forthcoming in future reports

## Recognition

Corey Payton – For his continued dedication to supporting application administration duties and spending the necessary time in excess of standard support hours and areas of responsibility to ensure our enterprise applications remain accessible and meeting the needs of our organization.

# SYSTEMS

PHIL MARQUEZ

## Accomplishments

- Completed Migration of Exchange data for active user mailboxes
  - o Supported missing email/calendar item issues after M365 cutover
  - o Project closeout in early May, but actual work completed in April.
- Began onboarding of Metallic cloud backup replacement for Commvault
  - o Install on servers and initiated backups on Dell NAS storage system
  - o Ongoing implementation meetings to get fully installed
- Multi-factor Authentication (MFA)
  - o Investigated use of Azure MFA for on premise applications like VPN and CAG
  - o Tested Azure MFA for on prem apps
  - o Created Pilot group for MFA and started using within select groups
- Confirmed Nessus scanning no longer impacts Nutanix cluster, specifically ECHO VMs, since the UH UCS cluster was rebuilt
- Working with NMTR to move them to Health Domain
  - o Initial task to bring them into our Globalscape SFTP service completed.
- Completed PEP evaluation discussions and submissions.
- Provided Systems support for Miners App for Dr. Sood

## In-Progress

- Continue investigation of issues with provisioning M365 licenses based on Job Title/Skill Code
  - o Waiting on main campus IT response
- Ongoing support of user questions about appropriate storage methods
  - o OneDrive, SharePoint, Teams, Azure (various offerings), and backup options
  - o Lots of confusion around available storage options as we begin to transition away from on premise network file shares.
- Ongoing testing of Azure MFA in pilot group

## Metrics

- System Availability – No systems unavailable
- Re-initiated Nessus scans – no impact

## Recognition

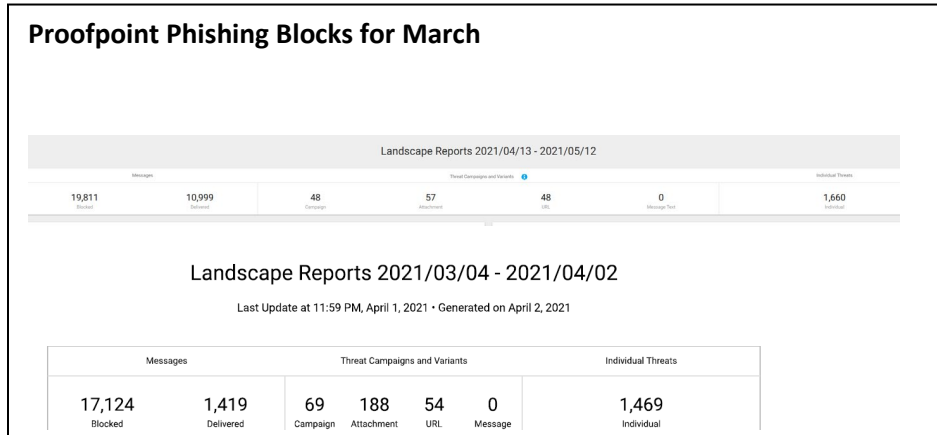
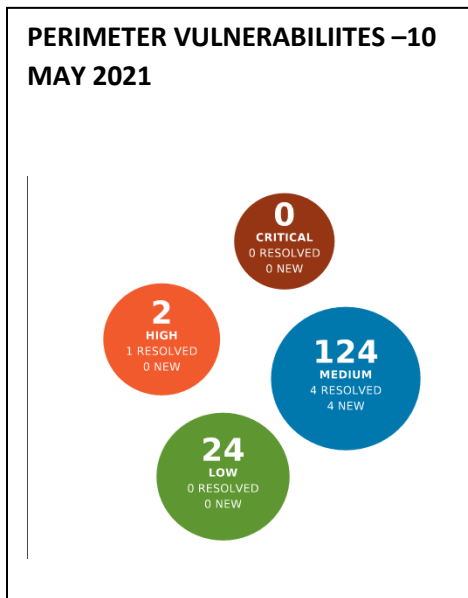
- The Help Desk(s) for supporting user issues and questions with M365.

# INFORMATION SECURITY

MIKE MEYER

## Accomplishments

ACTION	IMPACT
Continued to maintain very low vulnerabilities on public-facing devices and websites, especially for criticals and highs. Two new highs were due to a VPN vulnerability that will be patched shortly.	Criticals – Continues at 0 Highs - 2 (Increased from 0) Medium 124 (Decreased from 132)
Presented outbound email filtering results pertaining to PHI to the Privacy Officer. Discussed path forward.	Proofpoint has outbound filtering turned on now. We are seeing some email legitimately blocked for actual PHI. We need to develop processes to follow-up with individuals who make this mistake, such as training.
Root Cause Analysis (RCA) implemented in Cherwell service management system	Consistent, digitized RCAs are now submitted to and reviewed by Change Advisory Board and other stakeholders. A successful RCA program has been proved to reduce future outages by honest peer-review, pattern analysis and cultural change.
On 29 APR, began incident response to intrusion.	Responding to probable ransomware attack.
Root Cause Analysis	Incorporated changes recommended by Phil Marquez.



## In-Progress

PROJECT/ACTIVITY	PLANNED COMPLETION DATE	STATUS (Red, Yellow, Green)	NOTES
Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN	AUG 2021	Green	Completion date is best estimate based on recent events that have required large % of IT and security staff resources to respond to incident.
Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)	APR 2021 (for completion of policy and plan drafts for formal review as new HSC “cascaded” policy)	Complete Blue	Draft policy and strategy are 95% complete. NEXT STEPS: Provide draft of VM Strategy and policy to UH and HSC CIO. Brief ITSC, ITAC and ECC in April/May, then submit Core review via PAW.  Coordinated with PAW on process for making VM plan widely available to HSC stakeholders through Policy Manager.
Improve configuration management (Tom/Michael Schalip)	JUN 2021 (re-baselined)	Green	Work with stakeholders to improve our use of CMDB to manage hardware, software, dependencies, and backup/recovery POCs. Re-baselined due to additional scope and complexity.
Cyber Security Strategic Plan (Mike)	FEB 2021 (2021 Goals)	Complete*	Brief 2021 strategic objectives. Develop long-term plan to improve cyber posture.
	JUN 2021 (2022+ Goals) (re-baselined from APR)	Green	
Baseline Security Configuration for Windows (Zander)	2021 (Phase 2) June 2021	Green	Phase 2 of this effort determines how to implement the Windows 10 security baseline configurations in the imaging process based on best-practice standards. Phase 1 – Windows 10. Phase 2 – Windows Servers Phase 3 – IOS/Linux Phase 4 - Network devices

Analyze selected departments to determine how to increase workstation patching, encryption, and Windows 7 reduction	APR 2021	Green	<p>This has become a complex issue involving how we patch, what we patch and who is patching. May require additional training for sysadmins.</p> <p>CIO high-interest item assigned this month. Will work with other CIO elements to select sample departments. Goal is to determine what obstacles hinder hitting patching, encryption, and operating system security goals.</p>
Implement multi-factor authentication (MFA) for Microsoft 365	JUN 2021	Green	ISO assigned as accountable office for 365 MFA implementation. Project is on track currently.
Conduct Microsoft 365 security review	MAR 2021	Complete Blue	Review concluded that we must implement multi-factor authentication for due diligence protecting restricted and confidential information and getting to a "Low" risk. Review will be re-visited after MFA is implemented.
Issue new HSC Remote access policy. (Mike)	SEP 2020	Purple	<u>Deferred</u> due to other priorities.
Root Cause Analysis (RCA) process improvement (Tom/Mike)	JAN 2021	Complete JAN 2021	Aaron developed RCA template for Cherwell. Reviewed first RCA in CAB.
Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)	APR 2021 (for completion of policy and plan drafts for formal review as new HSC "cascaded" policy)	Complete APR 2021	

Baseline Security Configuration for Windows (Zander)	MAR 2021 (Phase 1)	Yellow	<p>Implement security baseline configurations in the imaging process based on best-practice standards. Phase 1 – Windows 10. Phase 2 – Windows Servers Phase 3 – IOS/Linux Phase 4 - Network devices</p> <p>Phase 1 has encountered some delays, missing the March target, but will complete in April.</p>
--	--------------------	--------	--

**METRICS**

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	<ul style="list-style-type: none"> <li>• 19 Data User Agreements/secure data transfer requests</li> <li>• 25 Software/Cloud App Purchases and Renewals</li> <li>• 6 Vulnerability Scans</li> <li>• 43 Other</li> </ul>	
NUMBER OF CONFIGURATION ITEMS PROCESSED	<ul style="list-style-type: none"> <li>• 9 Change Requests</li> <li>• 1 Root Cause Analysis (RCA)</li> </ul>	
SSL CERTIFICATES ISSUED OR RENEWED	<ul style="list-style-type: none"> <li>• 6 SSL certificates issued.</li> </ul>	
PERIMETER VULNERABILITIES	<ul style="list-style-type: none"> <li>• Criticals – 0 (Same as previous month)</li> <li>• Highs – 0 (Same as previous month)</li> <li>• Medium – 132 (Decreased from 137)</li> </ul>	

**Recognition**

The entire team of IT and security staff who reacted so quickly to the recent incident.

# TECHNOLOGY SUPPORT

RICK ADCOCK

## Accomplishments

- Switched Sailpoint from basic authentication to service provider authentication for azure connectors to support single sign on for HSC workstations.
- Started design process for move from HSC.AD “email policy” to Sailpoint management
- Demise Novell Netware Directory Services and modified all identity management services to work with Active Directory
- Hired a temp employee to assist with the O365 license change for 3500 HSC employees
- Continue to have Live Microsoft 365 training
- Developed and equipment replacement plan and budget for Health Sciences Rio Rancho
- Deployed Dragon fix to multiple HSC workstations

## In-Progress

- Testing multi-factor authentication and HSC workstation hybrid azure AD join for single sign on
- Hiring two Tier 1 IT service desk technicians
- Preparing to hire two other technicians for FY22
- Rebuilding the Cherwell schedule RABBITMQ services to get them stable
- Finish the clean-up of email transition related tickets
- Began moving 1500 of the 3500 HSC employee’s main campus O365 license from A3 to A1
- Developing a collaborative support model for multi-factor authentication with the Health System
- Preparing for an AV walk-thru of the new Center of Orthopedics Excellence in Rio Rancho
- Determining West Side IT Support for the entire Rio Rancho Campus
- Continued support of the GEER grant

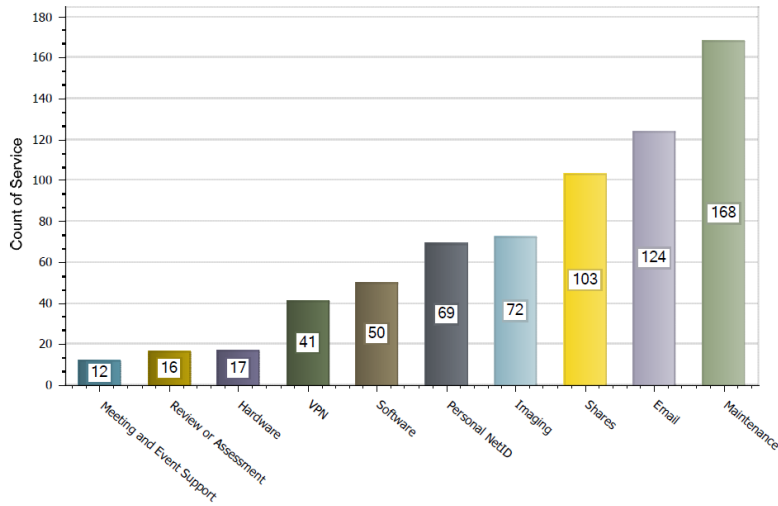


## Metrics

### Top 10 HSLIC Requests

04/01/2021 to 04/30/2021

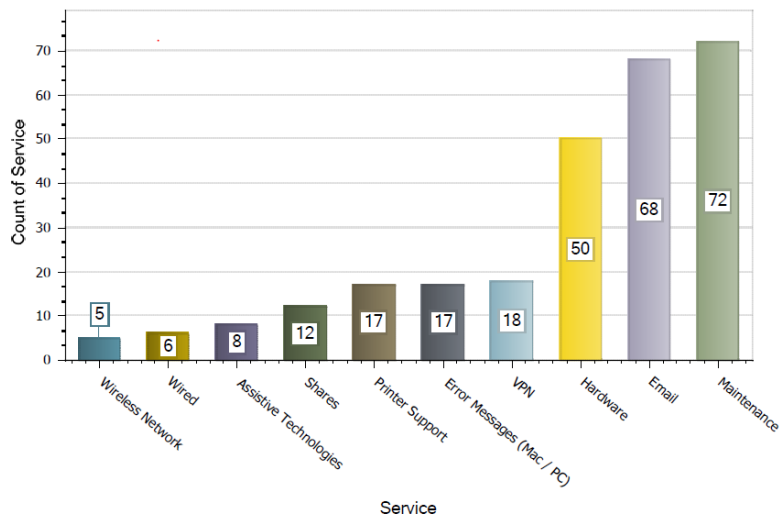
HSLIC By Service



### Top 10 Incidents - HSLIC

4/1/2021 to 4/30/2021

HSLIC By Service



## Recognition

Vernon Bell. Vernon has mostly single-handed managed the HSC IT Service desk phone support as the only Tier 1 technician in the group for the past month. We averaged 68.4 calls per day in April.

# UH IT NETWORK/NETSEC

CHARLIE WEAVER

## Accomplishments

- Much time devoted to incident management & response
- Multiple JNIS subteam activities in flight (Incident Management, Vulnerability Management, etc.)
- Azure MFA / Pulse integration confirmed
- InterVision engagement approaching conclusion
- Cancer Center access switch replacement completed
- NetSec Analyst candidate selected; offer pending
- UH / BBRP distribution switch replacement beginning
- HSC distribution switch replacement beginning
- UH outside facility / building EOL access switch replacements beginning

## In-Progress

- Century Link MOE capacity upgrade planned
- Wombat integration planning in process
- CAG MFA integration beginning

## Metrics

- TBD

## Recognition

- HSO ISO & Cyber Security team for outstanding teamwork