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
    - Supported missing email/calendar item issues after M365 cutover
    - Project closeout in early May, but actual work completed in April.
- Began onboarding of Metallic cloud backup replacement for Commvault
    - Install on servers and initiated backups on Dell NAS storage system
    - Ongoing implementation meetings to get fully installed
- Multi-factor Authentication (MFA)
    - Investigated use of Azure MFA for on premise applications like VPN and CAG
    - Tested Azure MFA for on prem apps
    - 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
    - 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
    - Waiting on main campus IT response
- Ongoing support of user questions about appropriate storage methods
    - OneDrive, SharePoint, Teams, Azure (various offerings), and backup options
    - 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.

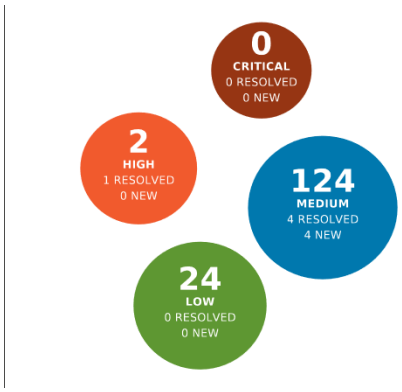
INFORMATION SECURITY

MIKE MEYER

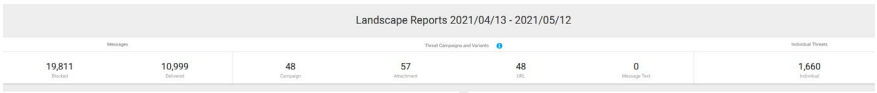
Accomplishments

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.

PERIMETER VULNERABILIITES –10 MAY 2021



Proofpoint Phishing Blocks for March



Landscape Reports 2021/03/04 - 2021/04/02

Last Update at 11:59 PM, April 1, 2021 • Generated on April 2, 2021

Messages		Threat Campaigns and Variants				Individual Threats
17,124 Blocked	1,419 Delivered	69 Campaign	188 Attachment	54 URL	0 Message	1,469 Individual

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	This has become a complex issue involving how we patch, what we patch and who is patching. May require additional training for sysadmins. 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.
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	Deferred 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	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 Phase 1 has encountered some delays, missing the March target, but will complete in April.

METRICS

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	• 19 Data User Agreements/secure data transfer requests • 25 Software/Cloud App Purchases and Renewals • 6 Vulnerability Scans • 43 Other	
NUMBER OF CONFIGURATION ITEMS PROCESSED	• 9 Change Requests • 1 Root Cause Analysis (RCA)	
SSL CERTIFICATES ISSUED OR RENEWED	• 6 SSL certificates issued.	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 0 (Same as previous month) • Medium – 132 (Decreased from 137)	

Recognition

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

TECHNOLOGY SUPPORT

RICK ADCOCK

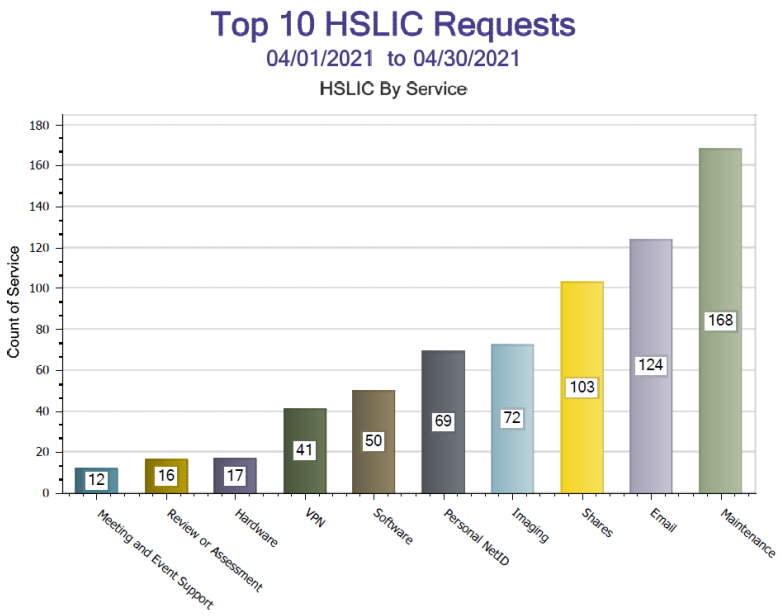
Accomplishments

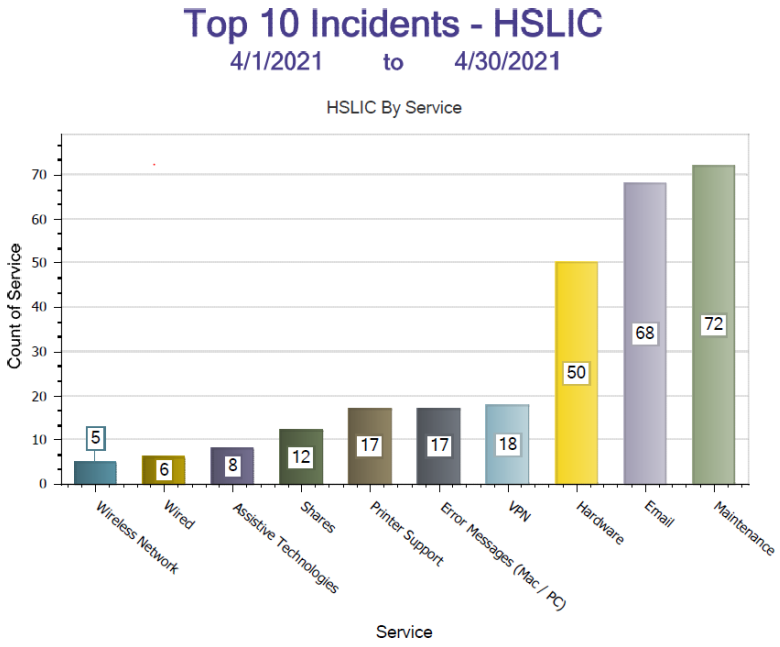
- Switched Sailpoint from basic authentication to service provider authentication for azure connectors to support single sign on for HSC workstations.
- Started design process for move from HSC.AD “email policy” to Sailpoint management
- Demise Novell Netware Directory Services and modified all identity 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





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 confirmend
- 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

HEALTH SCIENCES
CHIEF INFORMATION OFFICE

2021

1) **Security** first, then everything follows.

2) **Cloudification** with an emphasize on DR/BC and TCO.

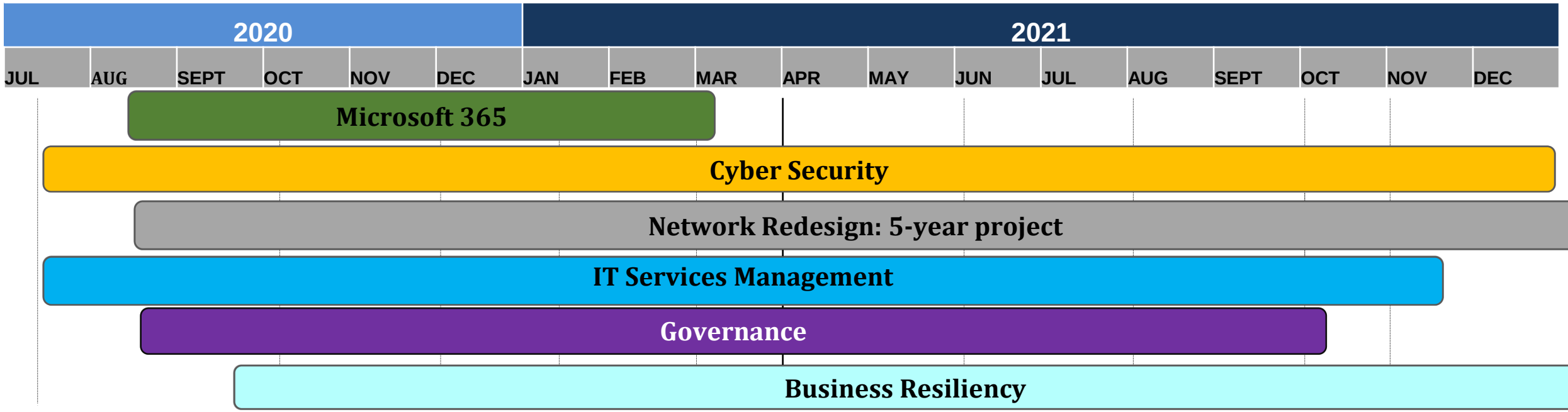
3) **Service Delivery** from our customers' perspective.

4) **Collaboration** with Microsoft 365 adoption.

5) **Network Modernization** 1st year of a 5-year transformation journey.

18-Month Strategic Roadmap

Marquez	Meyer	Weaver	Adcock	Sletten	Marquez
Microsoft 365	**Cyber Security**	**Network Redesign**	**IT Service Management**	**Governance/Policies**	**Business Resiliency**
~~1. Transfer domains~~	~~1. 6 KPIs~~	~~1. Requirements~~	~~1. 4 KPIs Dashboard~~	~~1. Charter for EIGC~~	1. Cloud strategy
~~2. Data migration~~	2. MFA M365	~~2. Network architect~~	~~2. Aging tickets Rpt~~.	~~2. Policy Manager~~	2. Backup/Recovery
~~3. Test~~	3. RCA process	3. Plan & Execute	~~3. Service Recovery~~	3. Update policies	3. Web Hosting
~~4. Training & Support~~	4. Vulnerability Assess	4. KPIs	~~4. Remote sup. tool~~	~~4. IT Website upgrade~~	
	5. Phishing program	5. Staff development	5. NPS survey/phone#		- - -
		6. Upgrade Internet	6. Single service portal		



1) **Communicate the Vision** to your team
want to play in the big games.

2) **Create the Roadmap** to where you wan
remember to celebrate wins along the jo

3) **Establish Metrics** to guide and light the
we measure, we improve.

Share your VRM

Start a Movement in 2021

https://www.youtube.com/watch?v=3EKAxQbYA9U

Lessons learned from M365 Migration – Feb 28

- **Our ecosystem is dirty**–there is **huge variation in computers, browsers, operating systems,** etc. We need to put a plan together for **standardization** across the enterprise and support model to align.

- There is a large **variation in technology savviness among our users**. We can setup a benchmark for the lowest common denominator for technology competence and train to that –could be win-win for both employees and organization.

- **Siloed culture,** even IT.

- Inadequate post Go-live Support, consider **outsource support** in light of the above points.

- Consider an **email retention policy.**

Other IT Supporting Initiatives in 2021

- Innovation Center Concept: Executive sponsor, Dr. Larson

- Project Hero – Broadband + Social determinants of health: Executive sponsor, Dr. Kaufman
  - One for the Intl Districts
  - Tohajiilee Navajo Reservation ~ ½ hour west of ABQ

- Teleworking Program: Executive sponsor, Kathy Agnew

- Microsoft 365 Adaption and Governance: IT Lead, Ray Avila