MAY 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
- Deployed unmhealth.org with external vendor
- Identity IQ/SailPoint training
- Provisioned 103 new Zoom Pro licenses
- Developed instructional materials for Radiology and SOM UME
- Conducted 5 Learning Central (LC) 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
Faculty Directory implementation	6/20/2021

Metrics

- SP2010 EOL activity tracking:
  - Total sites: 73
  - Awaiting assessment - 67
  - Migration to SPO in process – 3
  - Migration to alternative platform in process – 1
  - Requiring vendor assistance: N/A
  - Marked for deletion/abandonment: 2

SYSTEMS

PHIL MARQUEZ

Accomplishments

- Closed out Email migration project
- Began preparations for separated employee data migration

In-Progress

- Supporting security efforts across HSC CIO supported servers and storage
- Continued implementation of Metallic cloud backup across HSC servers
- Continued support for MFA testing on CAG

Metrics

- System Availability – No systems unavailable

Recognition

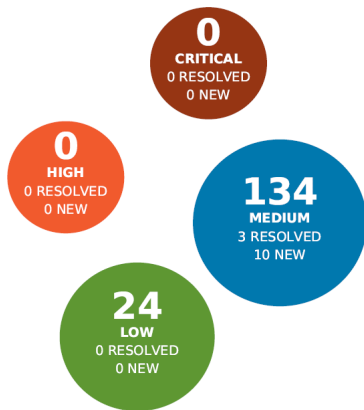- Mike Meyer for driving security efforts with a sane approach! Thanks, Mike.

INFORMATION SECURITY

MIKE MEYER

Accomplishments

ACTION	IMPACT
Most ISO resources focused on incident response in May.	Protect our data and network.
Continued to maintain very low vulnerabilities on public-facing devices and websites, especially for criticals and highs. The two highs in the last month's report are resolved.	Criticals – Continues at 0 Highs - 2 (Increased from 2) Medium 134 (Increased from 132)
New and improved Root Cause Analysis (RCA) tool implemented in Cherwell service management system based on inputs from Phil and his systems team.	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.

PERIMETER VULNERABILIITES

0
CRITICAL
0 RESOLVED
0 NEW

0
HIGH
0 RESOLVED
0 NEW

134
MEDIUM
3 RESOLVED
10 NEW

24
LOW
0 RESOLVED
0 NEW

Proofpoint Phishing Blocks for May

Messages		Threat Campaigns and Variants				Individual Threats
22,860 Blocked	6,035 Delivered	41 Campaign	128 Attachment	20 URL	0 Message Text	1,844 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	Red	On hold because resources working on incident. 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)	MAY 2021 – Brief ITAC, ECC, and EIGC so that policy and plan can be approved by core.	Yellow	Draft policy and strategy are 95% complete. NEXT STEPS: Provide draft of VM Strategy and policy to UH and HSC CIO. ITSC briefed. Brief ITAC and ECC in May, then submit Core review via PAW.
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
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.
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)	Complete	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.
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.
Issue new HSC Remote access policy. (Mike)	SEP 2020	Purple	Deferred due to other priorities.

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	• 5 Change Requests	
SSL CERTIFICATES ISSUED OR RENEWED	• 6 SSL certificates issued.	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 0 (Same as previous month) • Medium – 138 (Increased from 132)	

Recognition

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

TECHNOLOGY SUPPORT

RICK ADCOCK

Accomplishments

- Completed the main campus O365 licensing change for 3500 HSC employees
- Changed Tier 2 staff duties to support Tier 1 while two open positions are filled
- Moved Novell directory Services and on-prem Exchange domain out of reliance for SailPoint
- Migrated Email policy management off of on-prem exchange environment into SailPoint
  - Built additional support tools for email management
  - Identified path to tightly couple Azure Active Directory O365 data to identities
- Finished then clean-up of email related tickets for the transition to O365
- Develop a collaborative support model for multi-factor authentication with the Health System IT
- Completed the initial AV walk-thru of the new Center of Orthopedics Excellence in Rio Rancho
- Integrated the new OptiPlex 7090 model of workstations into the HSC standards, quotes, and Lobomart
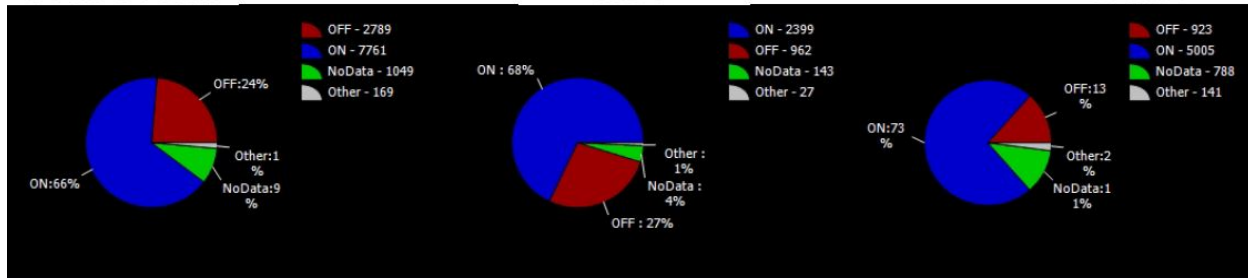- Deployed email caching for the Outlook client to improve the end user performance and experience

In-Progress

- NMTR Move to the Health domain
- Finish hiring two IT Support Tech 1 positions for phone support
- Preparing paperwork for two new IT Support Tech 2 positions for FY22
- Creating a unified IT support model for the Rio Rancho campus
- Testing multi-factor authentication and HSC workstation hybrid azure AD join for single sign on
- Resolving the workstation issues with McAfee and Carbon Black
- Determining West Side IT Support for the entire Rio Rancho Campus
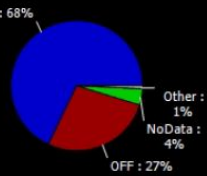- Continued support of the GEER grant
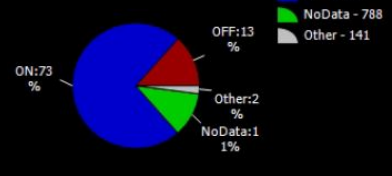
Metrics

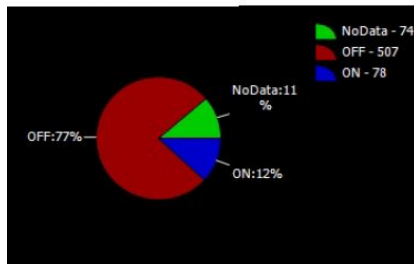### Encryption Report - Global

Total Overall

- OFF - 2789
- ON - 7761
- NoData - 1049
- Other - 169

OFF:24%
ON:66%
NoData:9%
Other:1%

HSC

- ON - 2399
- OFF - 962
- NoData - 143
- Other - 27

ON : 68%
Other : 1%
NoData : 4%
OFF : 27%

UNMH

- OFF - 923
- ON - 5005
- NoData - 788
- Other - 141

OFF:13%
ON:73%
Other:2%
NoData:1%

SRMC

- NoData - 74
- OFF - 507
- ON - 78

NoData:11%
OFF:77%
ON:12%

UNMMG

- OFF - 393
- ON - 274
- NoData - 44

OFF:55%
NoData:6%
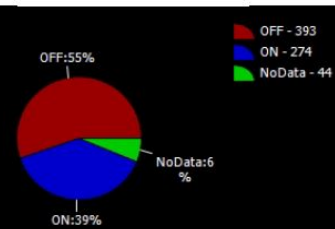ON:39%
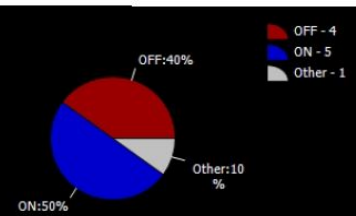
Unknown

- OFF - 4
- ON - 5
- Other - 1

OFF:40%
Other:10%
ON:50%

Recognition

I'd like to recognize Nick for stepping up to the challenge for only working here a short time, then becoming short-handed and personally filling the largest part of the void of the Tier 1 team. I know he can't wait to have additional staff, but his hard work is appreciated.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Most of the past month has been devoted to incident management & response
- Multiple JNIS subteam activities in flight (Incident Management, Vulnerability Management, etc.)
- NetSec Analyst candidate hired
- HSC & UH distribution switches racked, mounted, configured
- UH outside facility / building EOL access switch replacements beginning

In-Progress

- Century Link MOE capacity upgrade planned in process
- CAG MFA integration experiencing technical difficulties but planning rollout
- InterVision engagement approaching conclusion
- Juniper distribution switch replacements beginning

Metrics

- TBD

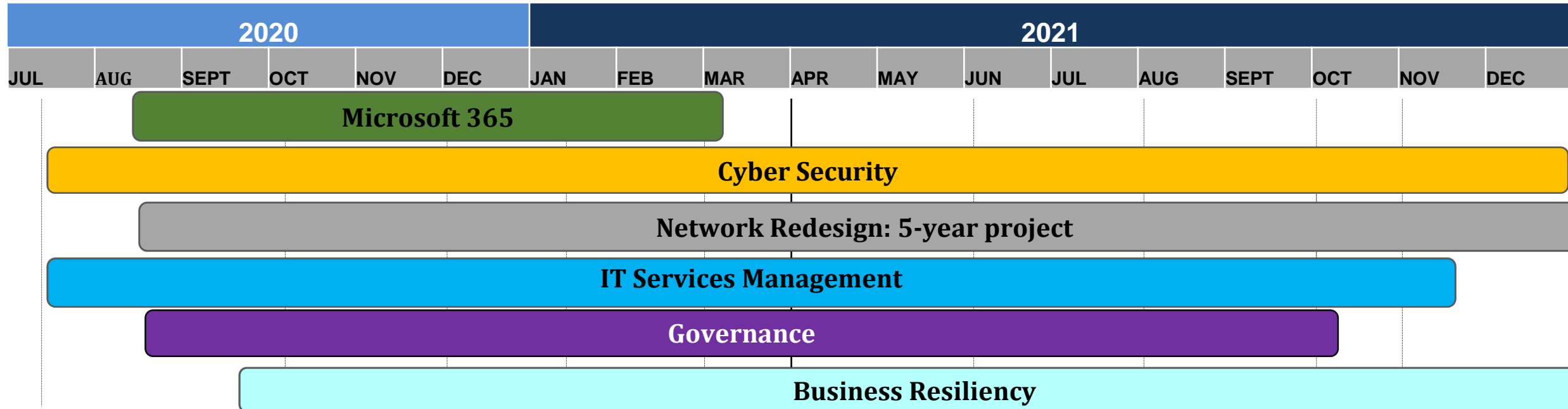## Recognition

- HSO ISO & Cyber Security team for outstanding teamwork

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		

2020	**2021**

JUL	AUG	SEPT	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC

Microsoft 365

Cyber Security

Network Redesign: 5-year project

IT Services Management

Governance

Business Resiliency

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

2) **Create the Roadmap** to where you wan[t] ... remember to celebrate wins along the jo[urney].

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

Share your VRM

IMAGINE A WORK PLACE WHERE EVERYONE ENGAGES AND CONTRIBUTES THEIR FULL INTELLECTUAL CAPACITY. A PLACE WHERE PEOPLE ARE HEALTHIER AND HAPPIER BECAUSE THEY HAVE MORE CONTROL OVER THEIR WORK- A PLACE WHERE EVERYONE IS A LEADER.

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