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

<table>
<thead>
<tr>
<th>Projects in flight</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint Online / m365 transition – Active</td>
<td>3/1/2022</td>
</tr>
<tr>
<td>Faculty Directory implementation</td>
<td>6/20/2021</td>
</tr>
</tbody>
</table>

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
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

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

In-Progress

<table>
<thead>
<tr>
<th>PROJECT/ACTIVITY</th>
<th>PLANNED COMPLETION DATE</th>
<th>STATUS (Red, Yellow, Green)</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN</td>
<td>AUG 2021</td>
<td>Red</td>
<td>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.</td>
</tr>
<tr>
<td>Task</td>
<td>Status</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Vulnerability management – Develop mature process to identify and</td>
<td>MAY 2021 – Brief ITAC,</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>track perimeter vulnerabilities and their mitigations (Michael</td>
<td>ECC, and EIGC so that policy and plan can be approved by core.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schalip/Zander)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve configuration management (Tom/Michael Schalip)</td>
<td>JUN 2021 (re-baselined)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Strategic Plan (Mike)</td>
<td>FEB 2021 (2021 Goals)</td>
<td>Brief 2021 strategic objectives. Develop long-term plan to improve cyber posture.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JUN 2021 (2022+ Goals)</td>
<td>(re-baselined from APR)</td>
<td></td>
</tr>
<tr>
<td>Conduct Microsoft 365 security review</td>
<td>MAR 2021</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Root Cause Analysis (RCA) process improvement (Tom/Mike)</td>
<td>JAN 2021</td>
<td>Aaron developed RCA template for Cherwell. Reviewed first RCA in CAB.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability management – Develop mature process to identify and</td>
<td>APR 2021 (for completion of policy and plan drafts for formal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>track perimeter vulnerabilities and their mitigations (Michael</td>
<td>review as new HSC “cascaded” policy)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schalip/Zander)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>METRIC</th>
<th>NUMBER</th>
<th>NOTES</th>
</tr>
</thead>
</table>
| 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 VULNERABILITIES | • 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
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.
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

<table>
<thead>
<tr>
<th>Marquez</th>
<th>Meyer</th>
<th>Weaver</th>
<th>Adcock</th>
<th>Sletten</th>
<th>Marquez</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft 365</strong></td>
<td><strong>Cyber Security</strong></td>
<td><strong>Network Redesign</strong></td>
<td><strong>IT Service Management</strong></td>
<td><strong>Governance/Policies</strong></td>
<td><strong>Business Resiliency</strong></td>
</tr>
<tr>
<td>5. Phishing program</td>
<td>5. Staff development</td>
<td>5. Update policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Upgrade Internet</td>
<td>6. Single service portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Microsoft 365

- Cyber Security
- Network Redesign: 5-year project
- IT Services Management
- Governance
- Business Resiliency

### Timeline

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUL</td>
<td>AUG</td>
<td>SEPT</td>
<td>OCT</td>
</tr>
<tr>
<td>NOV</td>
<td>DEC</td>
<td>JAN</td>
<td>FEB</td>
</tr>
<tr>
<td>MAR</td>
<td>APR</td>
<td>MAY</td>
<td>JUN</td>
</tr>
<tr>
<td>JUL</td>
<td>AUG</td>
<td>SEPT</td>
<td>OCT</td>
</tr>
<tr>
<td>NOV</td>
<td>DEC</td>
<td>JAN</td>
<td>FEB</td>
</tr>
<tr>
<td>MAR</td>
<td>APR</td>
<td>MAY</td>
<td>JUN</td>
</tr>
<tr>
<td>JUL</td>
<td>AUG</td>
<td>SEPT</td>
<td>OCT</td>
</tr>
<tr>
<td>NOV</td>
<td>DEC</td>
<td>JAN</td>
<td>FEB</td>
</tr>
</tbody>
</table>
1) Communicate the **Vision** to your team—remember people want to play in the big games.

2) Create the **Roadmap** to where you want to go—remember to celebrate wins along the journey.

3) Establish **Metrics** to guide and light the way—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 **outsourcing** 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