



HEALTH  
SCIENCES  

---

CHIEF INFORMATION  
OFFICE

## AUGUST UNIT REPORTS

APPLICATIONS-AVILA

PROJECT MANAGEMENT-SCHALIP

SYSTEMS-MARQUEZ

SECURITY-MEYER

TECHNOLOGY SUPPORT-ADCOCK

UNMH NETWORK-WEAVER

# APPLICATIONS

RAY AVILA

## Accomplishments

- a. Deployed Grief Services application
- b. Provided student information for resetting WEPA print credit system for fall semester
- c. Hired new PA3
- d. Identified and ended ongoing Azure charges for previously configured services that are no longer needed for ECHO, saving approximately \$3500/month.
- e. Collected and presented Zoom cloud storage analysis/info
- f. Finished additional branding in Telehealth login screen
- g. Contributed technical services toward a number of website deployments for HSC website redesign project
- h. Completed Cherwell CMDB automated upload process
- i. Deployed attestation-SHAC file transfer components
- j. Deployed Covid positive entry form

## In-Progress

Projects in flight	Status
Positive Covid student transfer to SHAC	9/9/2020
Automate monthly Zoom cloud storage analysis reports	9/11/2020
Develop Faculty Directory file transfer process from Digital Measures	9/30/2020
CTMS selection matrix	10/16/2020
Create DR/BC strategy SQL Server environment	12/31/2020
SSO/application entry consolidation	11/15/2020
Apps team customer portal	12/31/2020

Yellow are reflective of limited resources+short delivery dates

## Metrics

I didn't spend time planning to report on this section. I have numbers I can put together in coming week.

## Recognition

Ryan Jarvis should be recognized for having juggled his regular duties and the interim responsibilities during the course of the PA3 vacancy. During this time, he successfully delivered ASP.net solutions to customers, maintained the provisioning of Zoom, upgraded Moodle environment, restored and addressed issues with the SharePoint 2010 environment, had a large role in the deployment of the Zoom Telehealth environment and assisted in the Zoom Webinar requests, Zoom storage expansion, and research. There are other tasks he was able to deliver, but overall, I have a great appreciation for his efforts and his having assumed duties above and beyond.

# PROJECT MANAGEMENT

MICHAEL SCHALIP

## Accomplishments

- Outreach regarding CRICO implementation – will follow up with Erica/Wendy next week to figure out path forward
- Completed initial review of HSC IT policy spreadsheet
- Keeping the OMI/CMEv3 implementation on track
  - Facilitated demise of OMI's VPN – discussions and testing started
- Continued discussions with HSC IT Security

## In-Progress

- Policy reviews/entry – preliminary inventory is complete – will attempt to gather info on policies that are needed, but we don't have/own (some IT-related policies exist at UH level, but no equivalent policy exists at HSC-wide level)
  - We'll try to make quick work of this initiative
- Groundwork for BC/DR – finally getting some Systems info – will try to facilitate “next steps” in Cherwell/CMDB updates (need get Applications entries linked to Systems data)
- OMI CMS replacement – implement VertiQ/CMEv3
  - OMI has started using CMEv3 for mock “morning meetings” – going well, and good feedback

## Metrics

- I'll work on this

## Recognition

- Joe Fresquez and Jason Barnes – sys admin – efforts to inventory Systems' servers and identify owners/administrators

# SYSTEMS

PHIL MARQUEZ

## Accomplishments

### Personnel

- Bob Gagnon joined the group as an SNA3 from the Cancer Center
  - o Bob continues to support the Velos Upgrade for CC

### PRTG dashboard for OMI (Complete)

- Judson set up monitoring of OMI servers with notifications/alerts going to Martin Wetterstrom

### Nutanix Memory Expansion (Complete)

- We had plenty of CPU and Storage, but our memory utilization was running too high to make effective use of the other resources. Doubled memory across cluster (4 nodes) with no downtime.

## In-Progress

### Personnel

- Jacob Lujan resigned
  - o Network tech will likely not be backfilled. Other arrangement, Salary agreement, in discussion.

### Office 365 (In Progress)

- Created HSC O365 tenant working with Phil Main (TIG consultant)
- Mail domain release from UNM/add to HSC
- GAL synchronization options – Looked at various products/options including Microsoft Identity Manager. MIM is free and available, but complex with high overhead to install and maintain. Also, redundant to SailPoint. Agreed with UNM IT on CloudConnect product
  - o Forsyte IT, CloudConnect
    - Does everything we need and more that we want (sync guest accounts)
    - \$10,000/year
    - UNM IT already familiar with company and product
- Microsoft Licensing
  - o Multi-tenant amendment to MS contract to allow for HSC O365 tenant
  - o 5000 transitional SKUs (A3 licenses) loaded into the tenant

### Backup/Restore activities (focused on Ransomware prevention and/or recovery): (In Progress)

- Aaron and Judson – working on script to pull users from local admins on servers to audit for non-elevated accounts that have admin privileges.
- Inventory of servers and what's included in backups – Joe, Jason
- Challenge identifying all apps on departmental managed servers in our datacenter

- Phil met with Microsoft about cloud backup possibilities for central IT
  - o Waiting on proposals from Ms
- Jason completed a major Commvault version Upgrade and server virtualization

### Project ECHO – Grant for Covid-19/Nursing homes (In Progress)

- Request in progress for a new server for web reporting service
  - o VM built, Ubuntu OS, Nessus scan completed and remediations in progress - Joe
  - o Server to be externally accessible – use F5 for App Delivery – Judson/Joe
  - o quote to ECHO for hosting costs
- Teams for ECHO
  - o Built out disconnected local accounts in O365 for Project ECHO users
    - Teams ONLY will be provisioned to those accounts which will be [user@onmicrosoft.com](mailto:user@onmicrosoft.com) accounts with separate credentials. Accounts will be synced back up once identities are migrated over.

### **Metrics**

#### Downtime/Incidents:

- SimIQ SQL Server downtime
  - o Corrupted OS on SQL Server for Simulation IQ system. Data partition intact. Judson rebuilt the OS. Lewis reinstalled SQL and rebuilt database from backups. Took about 2.5 days, but were told the system wasn't need for a week. We used more time trying to recover since we had the time. Otherwise, would have simply rebuilt immediately - .5 day activity. Discussions ongoing about system hardening or recovery improvements.
- Poison Control (NMPDIC)
  - o Remote VPN router outage impacted one remote Pharmacist
  - o Single phone recording issue caused by user physically moving phone line
  - o Finally coordinate
- HSC DNS rebooted – no impact

### **Recognition**

- Judson Carter and Lewis Worley for recovery of SimIQ SQL Server

# INFORMATION SECURITY

MIKE MEYER

## Accomplishments

ACTION	IMPACT
Initiated CISA Perimeter Scans	Provides timely knowledge of vulnerabilities to external attack
Developed initial cyber security Key Performance Indicators (KPIs)	Ability to track progress and improvements in our cyber security posture
Participated on the Network RFP team, which just made a selection of a contractor	New network design is the first step toward building a 21 <sup>st</sup> Century secure network
Published first set of Cyber Security Key Performance Indicators	Measurement is the first step toward a first-class security program.
Encryption of Windows endpoints began	Better security posture, especially to protect HIPAA information and reduce HSC exposure to HIPAA penalties.

## In-Progress

PROJECT/ACTIVITY	PLANNED COMPLETION DATE	STATUS (Red, Yellow, Green)	NOTES
Issue new HSC Remote access policy.	SEP 2020	Yellow	Superseded by other priorities. May not make Sep.
Issue revised HSC Media and Device Handling policy	SEP 2020	Yellow	Superseded by other priorities. May not make Sep. Also, CIO issued compliance order for HSC devices ahead of policy change, lowering the priority.
ECHO Authorization to Operate from HHS for the AHRQ contract	SEP 15, 2020	Green	Last minute request, requires large level of effort to accomplish
Vulnerability management – Develop process to identify and track perimeter vulnerabilities and their mitigations	SEP 2020	Green	Because sysadmin responsibilities are often decentralized, we are lacking a basic notification process to send vulnerability items for patching. We also have not tracked open and closed vulnerabilities.

## Metrics

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	<ul style="list-style-type: none"><li>• 31 Data User Agreements</li><li>• 34 Software Purchases/Renewals</li></ul>	
NUMBER OF CONFIGURATION CHANGES PROCESSED	<ul style="list-style-type: none"><li>• 16</li></ul>	
PERIMETER VULNERABILITIES REDUCED	<ul style="list-style-type: none"><li>• Criticals – Decrease of 4</li><li>• Highs – Increased by 3</li></ul>	

## Recognition

Marsha Sletten for her great work on the Network Design RFP. She kept the process moving, did all of the “dirty work” like scheduling

# TECHNOLOGY SUPPORT

RICK ADCOCK

## Accomplishments

- Completed the transition from the legacy VPN to the new HSC vpn on August 3<sup>rd</sup>. The HSC is no longer using any VPN licenses from UNMH.
- Worked with main campus IT to get connected to their instance of the Apple School Manager in order to be able to manage Apple devices for the BYOD project.
- Completed and tested the requestable roles code in sailpoint. The framework is in place for any use cases that come up.
- Created an Organizational Unit for OMI and an OMI Admins group in the Health Domain. Added Martin Wetterstrom to the group in preparation for OMI to move workstations into the Health Domain.
- Acquired and implemented Beyond Trust Remote Desktop cloud service so we can remote into all desktops with an internet connection and not just those on our domain and network.
- Turned on encryption for the CIO container in active directory to force encrypt workstation within that container before turning on for other containers.

## In-Progress

- Reviewing and updating the change management training material for relevancy.
- Begging to map out the next phase of forced encryption to the department of Pediatrics container as long as we find no issues with workstations in the CIO container.
- Hiring a new IT support Tech 1 for the service desk.
- Looking at the possibility of obtaining a supervisor position for the service desk.
- Assisting OMI in setting up an HSC VPN specifically for them that will land then in their own DNS space. This will remove them from their proprietary VPN. After they migrate to the Health Domain we can have them move over to the standard VPN.
- Working with main campus IT to look into having Dell do the asset tagging of UNM/HSC purchased devices in order to eliminate issues with obtaining and deploying service tags which also causes inventory problems.
- Working with Judson to move Beyond Trust into our SAML authentication so we do not have to manage accounts for the service and make it easier to onboard other departments into our licensing.
- Working with the project team on the Center for Excellence in Orthopedics to be built next to SRMC. I am involved with possibly assisting with an RFP for an AV vendor, providing specifications, coordinating the installations, and doing verification testing. I will be using Chris Wray out there for the hands on things.

## Metrics

After 48 hours of turning on forced encryption on the CIO container:

- 74 objects – Total – CIO OU
  - 22 objects – No heartbeat (dead)
    - 1 of these is w7

- 52 Objects alive
  - 11 Encrypted
  - 41 Unencrypted
    - 19 TPM enabled
      - HW dates 8/25 – 8/13
      - Avg 6 days old
    - 2 TPM disabled
      - CIO000C29A68F8A
      - HSCF8CAB8051662
    - 20 No TPM status
      - HW dates 8/25-8/20
      - Avg 4 days old
- New HSC VPN (2000 concurrent licenses) has had a maximum concurrent usage of 394 concurrent users.

### **Recognition**

- Vernon Bell (HSC Service Desk) – As we have transitioned mainly to off-campus access, Vernon has been here every day assisting people over the phone with doing things remotely that they have never been done before. This is quite a steep learning curve for HSC employees and Vernon has quietly and effectively helped them navigate their way.

# UNMH NETWORK

CHARLIE WEAVER

## Accomplishments

- Performance reviews up to date
- ED switch reboot & RCA
- Network RFP finalization
- Cerner network migration & subsequent back-out
- NHT construction-related disaster mitigation planning completed

## In-Progress

- VPN / remote access core team (ongoing)
- Multiple administrative meetings
- Candidate interview for analyst position
- Projects
  - Cancer center network upgrade planning
  - Planning / prioritization for UH access switch upgrades
  - Internet Edge migration
  - Century Link MOE head-in planning
  - Cerner network migration retry
  - Network architectural redesign

## Metrics

- In development

## Recognition

- Mike Meyer & Scott Hanson on excellent collaboration & partnership on ongoing security concerns