JANUARY UNIT REPORTS

APPLICATIONS-**RAY AVILA**

PROJECT MANAGEMENT-**MICHAEL SCHALIP**

SYSTEMS-**PHIL MARQUEZ**

SECURITY-**MIKE MEYER**

TECHNOLOGY SUPPORT-**RICK ADCOCK**

IT NETWORK/NETSEC-**CHARLIE WEAVER**

HSC IT 2021 Vision

APPLICATIONS

RAY AVILA

Accomplishments

1) Accomplishments since last report
   - Go Live for Policy Manager and associated LDAP rule configurations successful
   - Completed Microsoft Azure Virtual Training: Fundamentals Part 1 and Part 2
   - Moodle Course development support and training
   - Learning Central Administration and training
   - Provisioned 158 Zoom licenses
2) Deployed 3 applications for testing to end-users

In-Progress

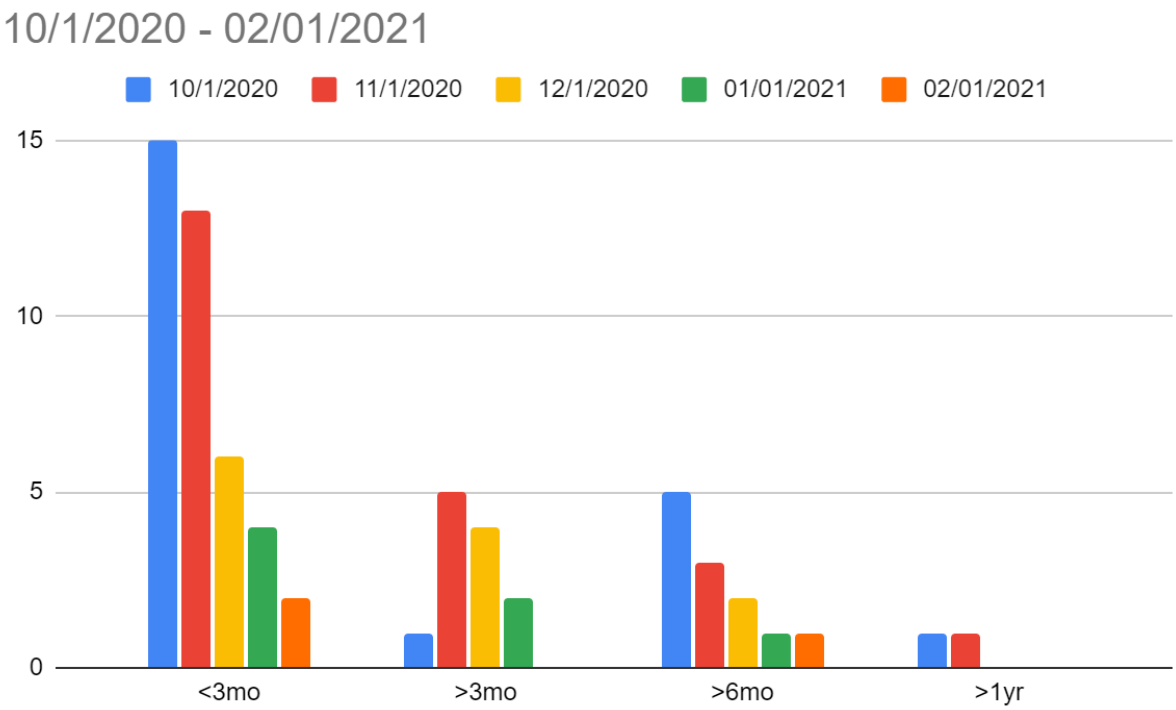
Projects in flight	Status
GWIM to MS Teams migration	3/27/2021
Sharepoint Online migration	6/1/2021
Faculty Directory	2/20/2021

Metrics

1) I will be creating new metrics from goals for the new year. The following is continued metric information for ticket aging. I will be replacing this metric for future months.

Reduction of longstanding open Cherwell tickets
Currently open tickets with age > 3 months
Currently open tickets with age > 6 months

	10/1/2020	11/1/2020	12/1/2020	01/01/2021	02/01/2021
<3mo	15	13	6	4	2
>3mo	1	5	4	2	0
>6mo	5	3	2	1	1
>1yr	1	1	0	0	0



Recognition

I-Ching. She has accomplished many tasks and initiatives in support of the HSC Website redesign, CMDB, and supported various .Net applications. She continues to be a great source of institutional knowledge and expertise. She has done so while working part time (20hrs/wk), and want to acknowledge her efforts and for being so productive and willing to help with all things asked of her.

PROJECT MANAGEMENT

MICHAEL SCHALIP

Accomplishments

- PEP Evaluation - Completed self-evaluation portion of my 2020 PEP
  - Will work with Roy and Mike Meyer to ensure that my 2021 goals are in alignment with the needs of the organization and the HSC ISO's Office.

In-Progress

- Vulnerability Management Strategy - work continues on the VM Strategy/Plan document. The plan will follow the 5-step cyclical process advocated by the "NIST Cybersecurity Framework" - "Identify, Protect, Detect, Respond and Recover". Work also continues on the parent "policy" document that will precede this "strategy" document. Met with some key stakeholder customers to assess their current VM processes, as well as any insights that they might have into the current UH/HSC vulnerability management processes/procedures - met with:
  - CCC/Ellan Jackson
  - UNMMG/Dick Weeda
  - Radiology/Jesse Bock & Donavan Goff
- Continue to engage with the HSC Policy Alignment working group to bring HSC IT policy up to date, (waiting for word on funding to bring in an experienced tech/policy writer to assist.

Metrics

- Incident Response process - continue to participate in ongoing discussions around improvement of the current IT incident response process.

Recognition

- None of note this month.

SYSTEMS

PHIL MARQUEZ

Accomplishments

- HSC M365 Migration – Status GREEN
    - Completed additional runs of incremental synchronizations of user mailboxes to gauge minimum amount of time to do the final runs prior to cutover.
    - Continuing ongoing migrations of additional Exchange objects including mailbox permissions, shared and resource mailboxes, contacts, and distribution groups.
    - Initiated migrations of Archived (data > 2 y.o.)
        - Approximately 40 TB of archive data – one time migration, static data
        - Archive mailbox migrations are on track to take about 15 days (in progress)
        - Incrementals will run after cutover to fix errors in migration data
    - Working on cutover task list to minimize impact of Go-Live
    - Biweekly *M365 Migration Status Update* meeting with key Stakeholders continued
        - Standard agenda:
            - Marquez – Migration status
            - Sletten – Communications plan/status
            - Adcock – Support and Training status
            - Avila – SharePoint and Instant Messaging (Teams) plan/status
        - Excellent attendance by stakeholders, customers, and departmental IT reps
- Provided PRTG monitoring to UNMH an SRMC systems in the wake of the SolarWinds compromise issue.
    - Made sufficient probes available to enable basic system and network monitoring while SolarWinds was out of commission.
- Progress continues on End of Support Windows 2008 servers

In-Progress

- Ongoing O365 migrations
    - Continue periodic incremental sync migrations for all user mailboxes
    - Complete Archive mailbox migrations
    - Finalize migrations of Shared mailboxes, resource mailboxes, distribution groups, permissions, etc.
    - Preparing User checklist/tasklist for items to check and do for use of new environment upon cutover to new environment. (R.Adcock team)
    - Finalize cutover task list for weekend of February 27-28. Cutover on Sunday morning. Most users will see new environment on morning March 1.
- Meeting with multiple vendors to review potential replacement for current Commvault Backup and Restore system
    - Most likely solution right now is a cloud solution from Commvault on Microsoft Azure
        - Full cloud solution, air-gapped backups for Ransomware protection
        - Avoid replacing all current on premise backup infrastructure
        - Avoid heavy labor load to manage and administer on premise backup infrastructure
    - Other vendor solutions considered include Dell/EMC

- Working with Microsoft and third party vendor on installing and running Movere cloud cost analysis tool
    - Jason installed and troubleshooting tool that estimates the cost of moving various/all compute loads to Azure

Metrics

- System Availability
    ~10 minutes impact to iECHO server during January, 5th Nessus scans

Recognition

- Jake Lujan and James Ankrum for quick response in getting PRTG monitoring set up for UNMH and SRMC respectively during SolarWinds compromise.

INFORMATION SECURITY

MIKE MEYER

Accomplishments

ACTION	IMPACT
Maintained very low vulnerabilities on public-facing devices and websites	Criticals – Continues at 0 Highs - 1 (Decreased from 2) Medium 127 (Decreased from 141)
Responded with NetSec and UH Cyber team to SolarWinds/SUNBURST worldwide attack.	Determined that our SolarWinds server received the compromised code. Disconnected server. Conducted hunt for other indications of compromise. Determined that HSC probably shut down its SolarWinds before attackers launched command and control phase and manual data exfiltration.
Completed DUA process improvement working group, including revision of forms, improvement of Privacy Office/ISO processes, identification of PI briefing opportunities.	By clarifying the forms that the PIs use, we expect to see a reduction in the time the various offices use to review DUAs and a decrease in complaints about processing times.
Completed ISO 2021 Strategic Goals* and briefed ITSC, HSC CIO Leadership and Managers' meetings, and other venues.	Provides priorities and direction for security efforts based on the need to reduce and manage risk.

PERIMETER VULNERABILIITES – 1 FEB 2021

In-Progress

PROJECT/ACTIVITY	PLANNED COMPLETION DATE	STATUS (Red, Yellow, Green)	NOTES
Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations	APR 2021 (Re-baselined from JAN 2021)	Green	We have expanded this effort from (1) process development and execution to (2) development of an enterprise Vulnerability Management Strategy for approval at the senior level and published in HSC

(Michael Schalip/Zander)			Policy Manager. These tactical and strategic efforts will run in parallel. Date has been re-baselined due to expanded scope. We will collaborate through the Joint Network and Information System (JNIS) team (NetSec, UH Cyber, ISO) to accomplish these goals for the entire enterprise.
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.
	APR 2021 (2022+ Goals)	Green	
Baseline Security Configuration for Windows (Zander)	MAR 2021 (Phase 1)	Green	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
Analyze selected departments to determine how to increase workstation patching, encryption, and Windows 7 reduction	APR 2021	Green	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.
Conduct Microsoft 365 security review	MAR 2021	GREEN	Review security options and settings to meet Microsoft and government best practices for "HIPAA compliance" when we transition to 365.
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.
Improve process for review of Data User Agreement (DUA)	DEC 2020	Complete JAN 2021	Under Privacy Officer's lead, stakeholders reviewed forms and processes to decrease

for research (Mike/Zander)			turnaround time for DUA processing.

* Read the 2021 ISO Strategic Goals . Adobe Acrobat Document

METRICS

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	• 16 Data User Agreements/secure data transfer • 33 Software/Cloud App Purchases and Renewals • 12 Vulnerability Scans • 58 Other	
NUMBER OF CONFIGURATION ITEMS PROCESSED	• 8 Change Requests • 1 Root Cause Analysis (RCA)	
SSL CERTIFICATES ISSUED OR RENEWED	• 3 (Kronos test, Inforcs and UH Air Watch)	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 1 (Decreased from 2) • Medium – 127 (Decreased from 141)	

RECOGNITIONS

I would like to recognize the DUA stakeholders' team, which met weekly for several months to find ways to improve the DUA approval process. All the members participated actively and contributed to improvements in the forms, in the processes and in the training for researchers to reduce confusions that can slow down the approval process. I especially want to recognize Laura Putz, our Privacy Officer, for her leadership in keeping the team on track. I also want to call out Hadya Khawaja in HRPO by name. Hadya led the documentation review in this endeavor and integrated dozens of change recommendation for the team's review. As a result, we simplified and clarifying many areas for the investigators completing these forms.

TECHNOLOGY SUPPORT

RICK ADCOCK

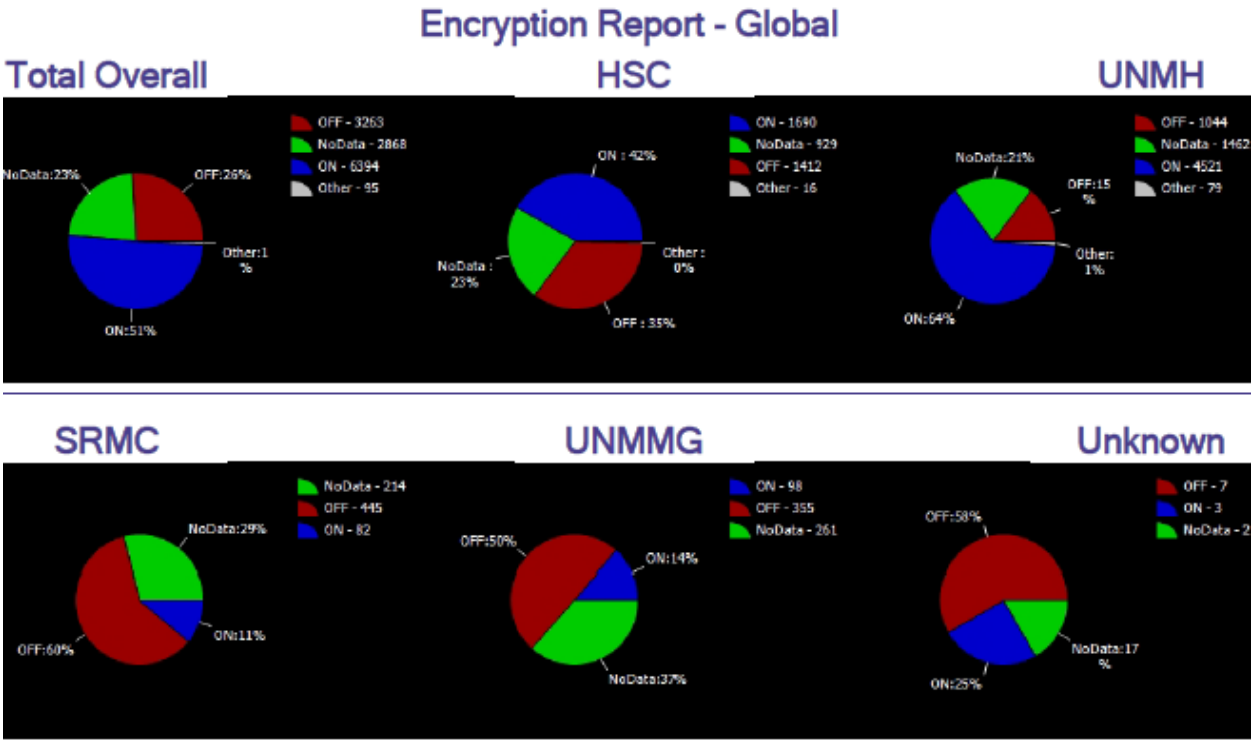
Accomplishments

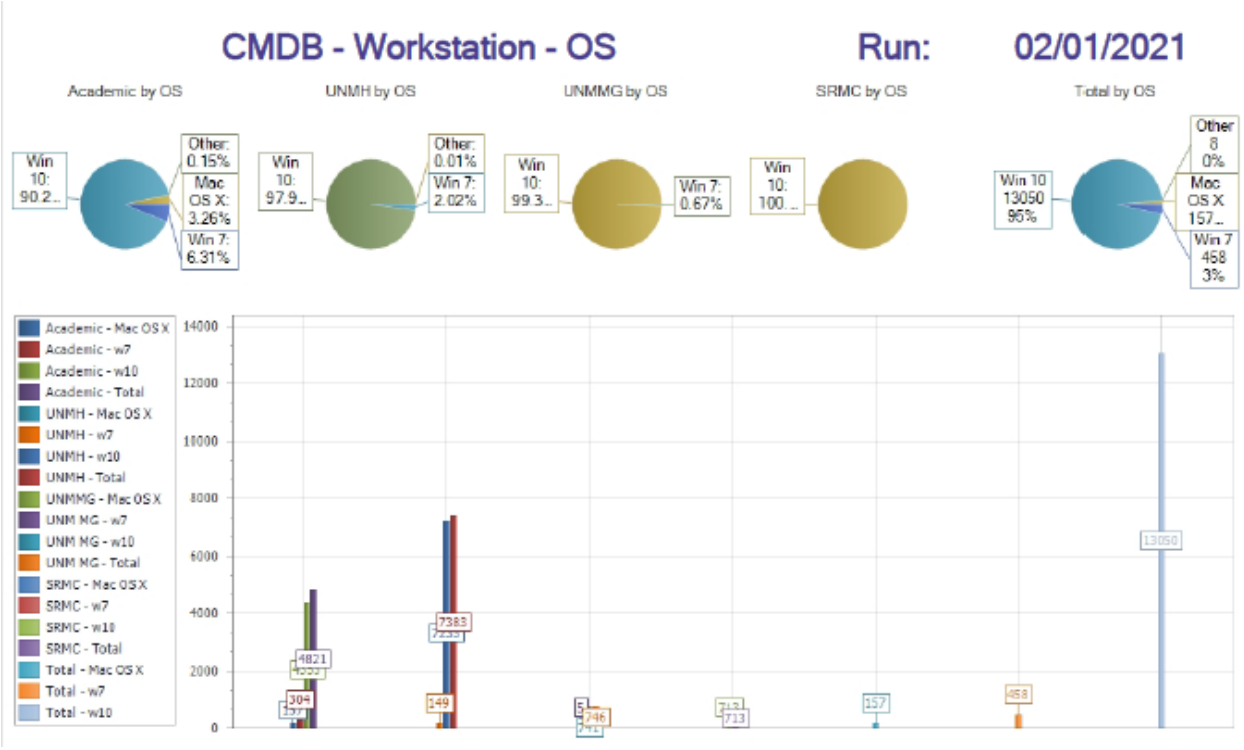
- Hired and on-boarded a Help Desk Supervisor
- Enabled forced workstation encryption on all HSC workstations
- Cherwell (Help.HSC) upgrade to version 10.1
- Upgraded AV in Fitz Hall 203 and 303
- Deployed Apple encryption for devices imaged from this point forward

In-Progress

- BYOD Support model and web page ready
- Live Microsoft 365 Training through February
- Microsoft 365 testing, pre go-live checklist development
- Working on support for Apple Big Sur operating system
- Working on imaging Apple devices with the proprietary M1 processor
- Modification to Sailpoint when Novell directory services are removed
- Orthopedics Center of Excellence AV equipment
- Exploring clientless detection tool to feed CMDB with software detection and dynamic linking
- Cherwell 10.2 upgrade
- Started overall design meeting for new Cherwell (Help.HSC) self-service portal
- Create a remediation process for workstations that do not automatically encrypt

Metrics





Recognition

Kyle Vick for the short turn-around on getting us a monthly data feed of HSC computer assets that have been surplused or deleted from inventory so we can remove those devices from out list of unencrypted workstations to remediate. This will save countless hours of tracking down devices that no longer exist.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Network outage management as required
- Phase 2 ProofPoint ESA completed
- Planning for multiple project requests for network team resources
- Capital budget development completed
- Operational budget requirements collection completed
- Wombat (ProofPoint) anti-phishing tool demonstration completed; recommendation to purchase.
- Gigapop link operational in preparation for internet edge migration
- Multiple lots of network replacement equipment received & inventoried
- InfoBlox (DNS / DHCP) server upgrade completed

In-Progress

- Century Link MOE capacity upgrade planned
- Network architectural redesign revisions requested
- UH access switch replacements in process
- Cancer Center access switch replacement project work underway
- Cerner inter-site circuit testing date in discussion
- Zayo / internet edge migration resources scheduled for a 3/10 – 12 migration.
- UH / BBRP distribution switch replacement in planning
- UH – SRMC Cerner circuit redundancy planning; tentatively scheduled 2/28/21
- High-level 2021 project planning
- ProofPoint Phase III deployment planning
- NetScaler MFA planning

Metrics

- TBD

Recognition

- HSO ISO & Cyber Security team for outstanding teamwork

HEALTH SCIENCES
CHIEF INFORMATION OFFICE

January 2021

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

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

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

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

5) **Network modernization** 1st year of a 4-year transformation journey.

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 take your team – remember to celebrate wins along the journey.

3) **Establish metrics** to guide and light the way - remember what we measure, we improve.

Share your VRM

Start a Movement in 2021

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