MARCH 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

- Worked with external vendor to get CCRA website migrated from Access DB to ASP.net/SQL Server
- HealthNM is recruiting for their summer programs. Made changes related to this, and added another program into the system.
- Coordinated with CCC to develop Velos data display
- Provided guidance and support of curriculum materials and Moodle administration
- Developed DOT/HAZMAT modules
- Additions to and modifications of existing CITI Covid-19 Back to work module
- Conducted LC training
- Provided additional configuration changes in Policy Manager to support power user roles
- Completed various m365 training courses
- Resolved various system issues

In-Progress

Projects in flight	Status
Sharepoint Online / m365 transition – Active	3/1/2022
Faculty Directory – Awaiting vendor testing	4/20/2021

Metrics

- New metrics starting in April will be gathered to measure legacy Sharepoint site migration

Recognition

I-Ching. In recognition of her work toward the HSC website redesign and continually providing great customer service.

SYSTEMS

PHIL MARQUEZ

Accomplishments

- Incremental syncs against active user mailboxes was completed
    - Ran targeted syncs to remediate missing item issues
- HSC mailbox archives migrated
    - Multiple runs of migrations against archive folders completed
- Purchased subscription to cover 160Tb of backup licensing with Commvault Metallic
    - Initial kickoff call with Metallic to initiate implementation
    - Planned solution is a cloud service from Commvault on Microsoft Azure
    - Full cloud solution, air-gapped backups for Ransomware protection
    - Avoid replacing all current on premise backup infrastructure
    - Avoid labor intensive management and administration of on premise backup infrastructure and tapes/tape libraries/tape storage

In-Progress

- Continue with post cutover migrations to get all data out of old exchange
    - Finishing up the Archive migration process through the month of April
- Continued work with vendor for installation of Metallic Backup and Restore
- Completed work with Microsoft and third party vendor on completing Movere cloud cost analysis tool
    - No specific actions to be taken based on analysis

Metrics

- System Availability – F5 unavailable for a few hours during issues with version upgrade
    - RCA in progress
- Delayed March 5 scheduled scans until April to continue troubleshooting and RCA.

Recognition

- The Help Desk(s) and others who supported the post cutover questions and issues
    - All involved in taking calls and answering questions after the O365 cutover.

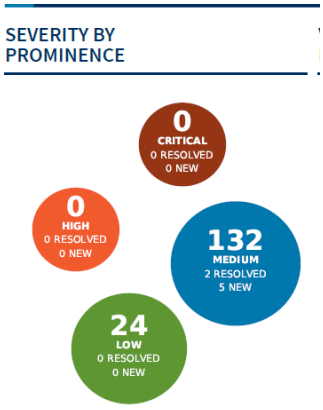
INFORMATION SECURITY

MIKE MEYER

Accomplishments

ACTION	IMPACT
Continued to maintain very low vulnerabilities on public-facing devices and websites, especially for criticals and highs	Criticals – Continues at 0 Highs - Continue at 0 Medium 132 (Decreased from 137)
Supported UH Cyber implementation of new Proofpoint module that checks web links in emails prior to delivery.	We have seen *significant* drop in malicious email links delivered. We believe this is a key reason why account compromises are down, and this reduces our ransomware exposure. (See metric below this table.)
Privacy Officer briefed the Executive Planning Committee on metrics after DUA process improvement recommendations were adopted between Privacy and Information Security Office.	Early results are a significant reduction of turnaround time for privacy and security reviews. Will continue to monitor and implement additional recommendation of the DUA process improvement WG.
"Vulnerability Outreach" by Mr. Schalip has engaged Facilities/Clinical Engineering, UH IT security, UH Network Security, Cancer Center and Physical Security.	Medical devices and other single-purpose devices such as security cameras are a major source of vulnerabilities in all organizations. We are raising awareness of this among the teams met and discovering that they also have concerns about vulnerabilities, especially medical devices like radiology equipment.
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.

PERIMETER VULNERABILIITES – 5 APR 2021



Proofpoint Phishing Blocks for March

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 (Michael Schalip/Zander)	APR 2021 (for completion of policy and plan drafts for formal review as new HSC "cascaded" policy)	Green	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)	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.
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.
Improve process for review of Data User Agreement (DUA) for research (Mike/Zander)	DEC 2020	Complete JAN 2021	Under Privacy Officer's lead, stakeholders reviewed forms and processes to decrease turnaround time for DUA processing.

METRICS

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	• 17 Data User Agreements/secure data transfer requests • 21 Software/Cloud App Purchases and Renewals • 8 Vulnerability Scans • 42 Other	
NUMBER OF CONFIGURATION ITEMS PROCESSED	• 11 Change Requests • 1 Emergency Change – blocked emails from a known bad actor from an overseas address • 3 Root Cause Analysis (RCA)	
SSL CERTIFICATES ISSUED OR RENEWED	• 9 SSL certificates issued	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 0 (Same as previous month) • Medium – 132 (Decreased from 137)	

TECHNOLOGY SUPPORT

RICK ADCOCK

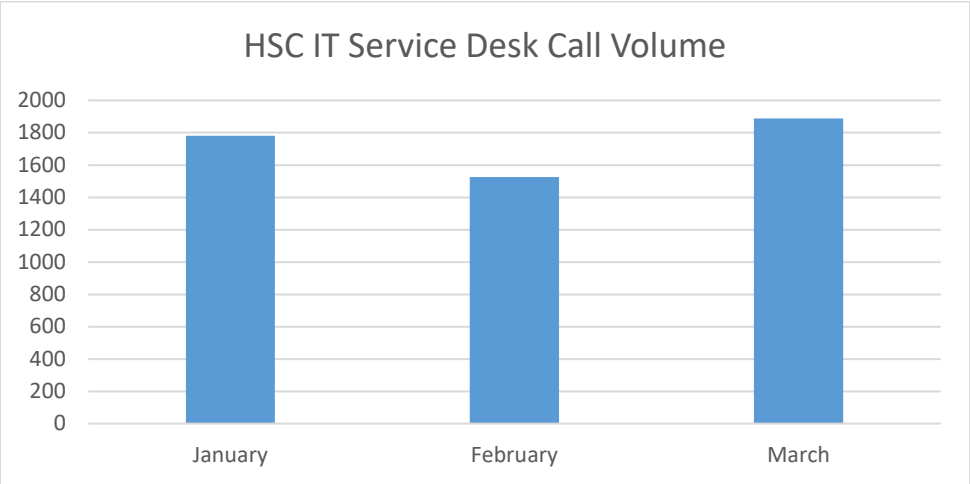
Accomplishments

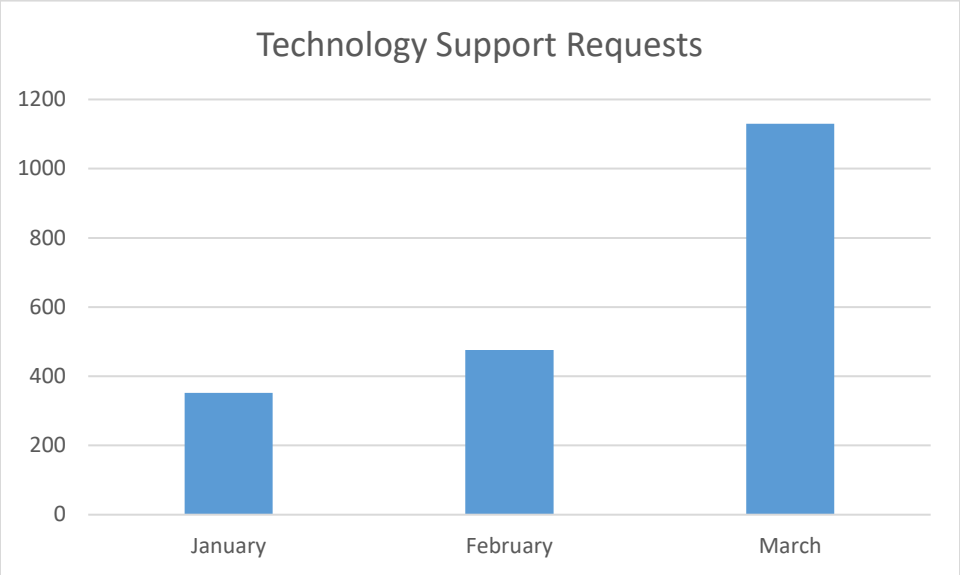
- Created a new enterprise standard Apple workstation image for devices that have the new M1 processor.
- Supported the O365 project for the majority of this month.
- Sustained a queue of ~300 tickets, and to date we are holding under an average of 20.
- Triaged and resolved nearly 1000 requests from the email migration.
- The team identified several systematic technical problems and developed PowerShell scripts to resolve some, other we use the automation tools we manage to build in additional solutions.
- We supported all Organizational groups and Service desks with any project related issue, to allow those groups to move into a support position for their organization at the speed they required.
- Published an installer package for Microsoft Access 2019 in Software Center.
- Implemented a group policy for domain joined workstations participating in the MFA pilot to do single sign-on from workstation browsers.
- Hired a temp employee to support the change in MS365 licensing on main campus from A3 to A1 for HSC employees.
- Began GEER grant equipment checkout – 12 checkouts in first week.

In-Progress

- Developing Soft-Skill Guide for the HSC IT Service Desk agents.
- Starting shadowing service desk agents with Tier 2 technicians to help develop staff and ensure standards for triage prior to escalating requests.
- Working on establishing expectations for ticket creation and closure, will set criteria for ticket creation for small issues, pw reset etc.
- Finalize hiring a service desk agent.
- Four HSC classroom upgrades.
- Onboarding more faculty to Mediasite/Zoom storage – currently working with OT and EMS.
- Developing a process for moving old Zoom content to Mediasite.
- New classroom upgrades underway in Domenici, Pharmacy, and Public Health buildings to add active learning and hybrid classroom support.

Metrics





Recognition

Fisher Lovett from the HSC IT Service Desk. Fisher has handled the majority of the phone calls at the helpdesk during the email transition along with the normal work load. Fisher maintained and very positive and upbeat attitude and work effort throughout the surge of incoming calls.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Final segment of the Zayo/Internet edge migration completed
- Multiple JNIS sub-team activities in flight (Incident Management, Vulnerability Management, etc.)
- UH EOL access switch replacement completed
- Cancer Center access switch replacement past the halfway point
- Wombat selected as the next-gen anti-phishing tool. Contract with purchasing.
- Network Tech hired
- NetSec Analyst position posted; reviewing candidates
- Pulse/CAG Azure MFA evaluation commencing
- UH/BBRP distribution switch replacement process beginning
- Initial evaluation of Medigate medical device scanning tool completed; awaiting quote
- ISE equipment placement & evaluation beginning

In-Progress

- Century Link MOE capacity upgrade planned
- Wombat integration planning in process
- Completion of Cancer Center access switch replacements in sight
- HSC distribution switch replacements beginning
- UH outside facility/building EOL access switch replacements beginning

Metrics

- TBD

Recognition

- HSO ISO & Cyber Security team for outstanding teamwork