DECEMBER UNIT REPORTS

APPLICATIONS-**RAY AVILA**

PROJECT MANAGEMENT-**MICHAEL SCHALIP**

SYSTEMS-**PHIL MARQUEZ**

SECURITY-**MIKE MEYER**

TECHNOLOGY SUPPORT-**RICK ADCOCK**

UH IT NETWORK/NETSEC-**CHARLIE WEAVER**

APPLICATIONS

RAY AVILA

Accomplishments

- Deployed BREP Mentorship SSRS report
- Updated Interpersonal Violence report dataset
- Coordinated with main campus to update Clinical rotation data to infection control
- Updated Backup support process for Attestation
- Continued HSC website redesign support adding redirects, debugging, etc
- Moodle and Learning Central curriculum development, training and support
- Implemented Policy Manager notification email Banners
- Provisioned 99 new Zoom licenses

In-Progress

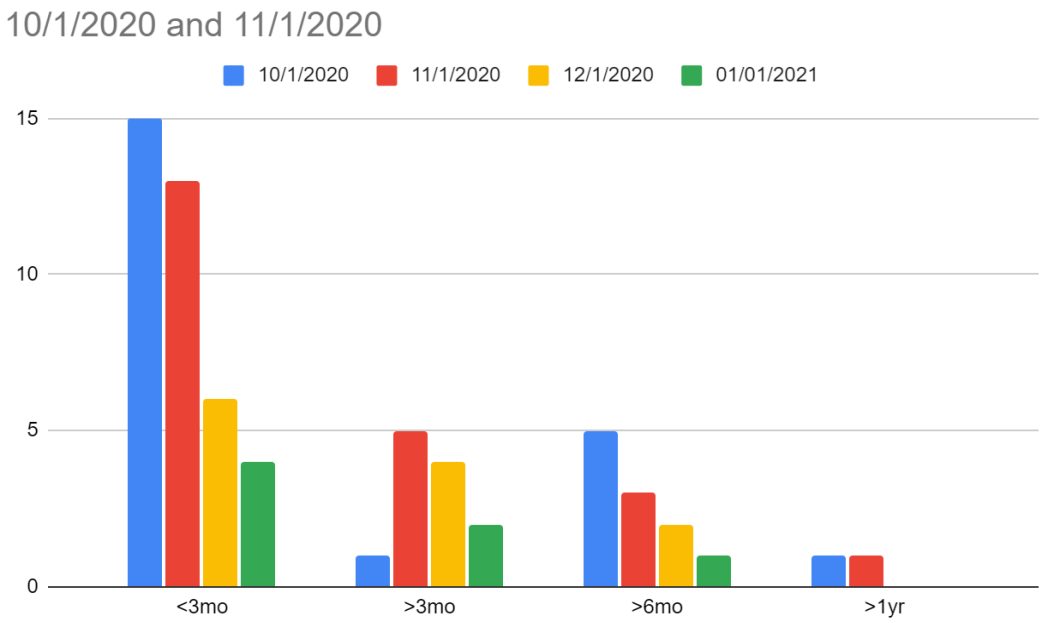
Projects in flight	Status
GWIM to MS Teams migration	3/14/2021
Sharepoint Online migration	6/1/2021

Metrics

The objective driven by this metric has largely been met (Reduction of longstanding open Cherwell tickets).
I will be creating new metrics from goals for the new year. The following is continued metric information for ticket aging. I will probably 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
<3mo	15	13	6	4
>3mo	1	5	4	2
>6mo	5	3	2	1
>1yr	1	1	0	0



Recognition

Laura Day. Laura has helped me and my team with numerous administrative matters over the course of the past year during COVID. She has always been professional, patient, and easy to work with. Despite the many additional duties that I observe her assuming, she has always been timely and proficient with all matters that I work with her on.

PROJECT MANAGEMENT

MICHAEL SCHALIP

Accomplishments

- Beginning work with HSC IT Security – under the direction of Mike Meyers/HSC ISO, I will be partnering with IT Security to expand/improve their operational capabilities. I will participate and consult with Mike Meyer as necessary. Currently reviewing ISO's ongoing priority list (with Mike) to see where I can be of assistance.
  - Next steps: Highest priority for ISO's Office right now is documenting/implementing an enterprise-wide vulnerability management program/process. Will hopefully define targets and milestones in Jan/Feb 2021.
- The CRICO implementation (CRICO is the Harvard-based insurance consulting program engaged by HSC Legal) appears to be moving forward. We will continue to monitor the project and assist as necessary.
- Continue to communicate with HSC IT Systems and Applications folks, as well as some of the educational techs regarding use of the Cherwell CMDB capability to track software applications running on HSC compute resources. Tom Gutierrez/IT Security has started reviewing sample Cherwell reports. He should have some sample reports ready by January.
- Continue to implement PolicyManager for HSC IT policies – will continue to work with HSC IT personnel to get existing policies moved from the spreadsheet in to the PolicyManager system
  - Challenge: While PolicyManager is a centralized system – it's apparent that all the different stakeholders have differing ideas on exactly how to configure and implement the PM system.
- The OMI/CMEv3 implementation is reportedly on track.
  - Since most OMI/CMEv3 implementation work has been assumed by OMI's own core project team, HSC IT will be contacted if information/support is necessary.

In-Progress

- Beginning work with Mike Meyer/ISO to begin developing a formal, HSC-wide IT security vulnerability management program. Discussions have started and we're developing a scope and plan to move this forward. (We're anticipating that majority of my time this year will be spent on HSC IT security initiatives and assisting the ISO's Office.)
  - Challenge: We have to make sure that both HSC IT, Networking and UH IT security teams work in unison on this initiative. Broader and less restrictive access to some of our existing IT security tools/systems will be required. Endorsement by the HSC CIO, and UH IT leadership, will help move this enterprise-wide effort forward.
  - Current work being done on the Cherwell CMDB will be leveraged directly into this ongoing effort. Inventories of hardware and software will be imperative to any future vulnerability processes.
- Policy reviews/entry – continuing 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)
  - PolicyManager will be "in production" mid-January 2021. We're working to get all HSC IT policies into the PM system now.
- OMI CMS replacement – implement VertiQ/CMEv3

- OMI continues their implementation of CMEv3 – testing continues to go well, per Martin Wetterstrom/OMI IT

Metrics

- Proposed: As we move the IT Security vulnerability management program forward – we're anticipating that there will be a number of valuable metrics to work from.
- Proposed: Policy review progress?
  - Number of HSC IT policies complete/up to date: 1
  - Number of HSC IT policies in progress/under review: ~16
- Proposed: Cherwell/CMDB update progress? (As soon as we get more production data into the Cherwell CMDB – we'll start distributing reports. Hopefully we'll be able to start mining some data – and metrics – from these CMDB reports.)
  - Number of IT applications being hosted on HSC IT systems: ??
  - Number of IT applications being tracked in Cherwell/CMDB: ??

Recognition

- None of note this month.

SYSTEMS

PHIL MARQUEZ

Accomplishments

- HSC M365 Migration – Status GREEN
  - Began initial migrations of additional Exchange objects including mailbox permissions, shared and resource mailboxes, contacts, and distribution groups.
  - Planning/preparations to migrate Archived (data > 2 y.o.)
    - Approximately 40 TB of archive data – one time migration, no incrementals
  - Working on cutover strategy 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
- Progress continues on End of Support Windows 2008 servers
  - Work continues with departmental owners to migrate to supported OS version

In-Progress

- Ongoing O365 migrations
  - Continue periodic incremental sync migrations for all user mailboxes
  - Finalize migrations of Shared mailboxes, resource mailboxes, distribution groups, permissions, etc.
  - Identify cutover process and date
- Meeting with multiple vendors to review potential replacement for current Commvault Backup and Restore system
  - Update current Commvault with new offerings for BAR
  - Other vendor solutions including Dell/EMC

Metrics

- System Availability
  - Zero unscheduled downtime (Dec) – Servers/Storage

Recognition

- Bob Gagnon for willingness to continue data migration activity over the Winter break. Thanks, Bob!

INFORMATION SECURITY

MIKE MEYER

Accomplishments

ACTION	IMPACT
Improved perimeter security by closing more vulnerabilities.	Criticals – Continues at 0 Highs - 3 > 2
Collaborated with UH Security and NetSec to deploy Proofpoint in record time	Vastly improved scanning of inbound email. Data Loss Prevention capability.
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.

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 (Zander/Michael S.)	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 Plan for approval at the senior level and published in HSC Policy Manager. These tactical and strategic efforts will run in parallel. Date has been re-baselined due to expanded scope. 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.
Improve configuration management (Tom/Michael Schalip)	DEC 2020	Green	Work with stakeholders to improve our use of CMDB to manage hardware, software, dependencies and backup/recovery POCs.
Cyber Security Strategic Plan (Mike)	FEB 2021 (Re-baselined from NOV 2020)	Yellow	Develop long-term plan to improve cyber posture.

			Re-baselined from Nov 2020 to Feb 2021
Improve process for review of Data User Agreement (DUA) for research (Mike/Zander)	DEC 2020	Green	Under Privacy Officer's lead, stakeholders are reviewing forms and processes to decrease turnaround time for DUA processing.
Baseline Security Configuration for Windows (Zander)	MAR 2021	Green	Implement security baseline configurations in the imaging process based on best-practice standards. Phase 1 – Windows 10. Phase 2 – Windows Servers and Network devices
Root Cause Analysis (RCA) process improvement (Tom/Mike)	JAN 2021	Green	Implement a process for conducting and reviewing RCAs using the existing CAB and Cherwell.
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.
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 • 36 Software Purchases and Renewals • 17 Vulnerability Scans • 38 Other	
NUMBER OF CONFIGURATION CHANGES PROCESSED	• 7	
SSL CERTIFICATES ISSUED OR RENEWED	• 1	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 2 (Decreased from 3) • Medium – 141	

RECOGNITIONS

Meghann Carrillo, Francisco Cordoba and Scott Hanson (NetSec) for their rapid deployment of the Proofpoint email filter. They deployed this new capability in several weeks, when such a major effort would normally require at least a few months. Proofpoint significantly increasing our protection against email-borne malicious attacks. Even though they executed quickly, there was no disruption of email services to HSC customers.

TECHNOLOGY SUPPORT

RICK ADCOCK

Accomplishments

Hired new IT Support Tech 1 for the Service desk

Added FAQ to the MS 365 web page and uploaded training videos

Completed the Cherwell 10.1 upgrade

Completed and documented December Microsoft 365 trainings

In-Progress

Interviewing for new position Technical Support Analyst 1 as a supervisor of the HSC Service Desk.

HSC-wide forced encryption of workstations to begin January 7, 2021

BYOD Support model and web page ready

Looking at the technical aspects of moving NMTR into the HSC Health Domain

Established Live Microsoft 365 Training through January

Developing Image process for new Apple Hardware

Working though issues with the new Apple operating system “Big Sur”

Metrics

December 1 - 23 2019 818 support calls / 41 per day average

December 1 – 23 2020 1148 support calls / 50 per day average (+40.34%)

December 2019 (HSC Tier 1 and Tier 2) tickets 395

December 2020 (HSC Tier 1 and Tier 2) tickets 264 (-33.16%)

Recognition

Rob Cole for the excellent work in upgrading Cherwell

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Network outage management as required
- SolarWinds incident management consumed much time over the past month
- Access switch replacements at SRMC placed and ready to deploy
- Phase 2 ProofPoint ESA integration planning completed
- Planning for multiple project requests for network team resources
- Network architectural redesign BOM & associated costs delivered for budgetary development
- Wombat (ProofPoint) anti-phishing tool demonstration completed
- Multiple COVID-related surge activities completed
- Malware & phishing organizational awareness communications developed & delivered in partnership with HSC ISO

In-Progress

- Network architectural redesign revisions requested
- UH / BBRP distribution switch replacement
- InfoBlox (DNS / DHCP) server upgrade
- Budget completion for next FY
- UH – SRMC Cerner circuit redundancy planning
- Cancer Center access switch replacement to commence
- High-level 2021 project planning
- Email phishing management tool evaluation
- ProofPoint Phase II deployment (outbound mail & secure email end-user changes)
- NetScaler MFA planning

Metrics

- TBD

Recognition

- HSO ISO & Cyber Security team for SolarWinds response.