FEBRUARY UNIT REPORTS

APPLICATIONS - RAY AVILA
PROJECT MANAGEMENT - MICHAEL SCHALIP
SYSTEMS - PHIL MARQUEZ
SECURITY - MIKE MEYER
TECHNOLOGY SUPPORT - RICK ADCOCK
NETWORK/NETSEC - CHARLIE WEAVER

HSC 2021 VISION
Accomplishments

- Launched the IPE Honors database
- Prepped and deployed FY22 FIBCI system
- Student scheduling for the MD classes of 2023 and 2024
- Made changes to the HealthNM website, they are re-launching for 2021 summer
- Fixed issues with TriNetX loader and got latest load done
- Developed SSIS package to load faculty directory data from web services
- Provisioned 134 Zoom Pro License Accounts
- Provisioning and application administration for Trinetx
- Completed Microsoft Mechanics Training
- Developed DOT HazMat course materials
- Various administrative tasks with CITI Covid-19 Back to Campus course
- Learning Central and Moodle administration tasks
- Conducted Training for Faculty and Staff for Moodle
- Provided Zoom support for M365 deployment

In-Progress

<table>
<thead>
<tr>
<th>Projects in flight</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>GWIM to MS Teams migration</td>
<td>3/27/2021</td>
</tr>
<tr>
<td>Sharepoint Online migration</td>
<td>6/1/2021</td>
</tr>
<tr>
<td>Faculty Directory</td>
<td>2/20/2021</td>
</tr>
</tbody>
</table>

Metrics

- 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

Recognition

Kyle Vick for his consistent and exceptional support for the School Medicine. I can always be confident that his work is thorough, of high quality and timely. He anticipates and addresses potential problems, and has developed a strong business relationship with the school. It’s because he addresses things so well that we often don’t hear from his area too much, but his work should be recognized.
ACCOMPLISHMENTS

  - Worked with both Roy and Mike Meyer to align my 2021 goals with the needs of the organization, the HSC CIO 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 HSC ISO. The draft plan is ~80% complete, and should be ready for wider review sometime in March. Work also continues on the parent “policy” document that will precede this “strategy” document.
- Met with another key stakeholder 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:
  - Facilities/Rico Valpato & Richard Crise – they are interested in continuing discussions regarding vulnerability assessments on equipment managed through Clinical Engineering (outsourced to Trimedx – they maintain most clinical hardware). They are also interested in discussing vulnerability questions regarding their plant/HVAC equipment.
  - Physical Security/Robert Talley, Vito Capobianco and Robert Perry – discussed implications for physical security systems, cameras, alarms, etc. They would like to expand their dialogue.
- 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.)
- Continue to participate in the HSC/Joint Network & Information Security committee as a non-voting member.
- Incident Response process - continue to participate in ongoing discussions around improvement of the current IT incident response process.

METRICS

- I’ll have to work with HSC ISO to identify appropriate metrics to be reporting out.

RECOGNITION

- I’d like to acknowledge Marcia Sletten for putting forward the idea of a Zoom “support room” during the first few days of the M365 deployment. It was a great idea that customers clearly appreciated.
I’d like to acknowledge Brent Ellison from UH/CTL. Brent was key in overseeing the customer intake in the Zoom “support room” during the M365 migration. His positive attitude and customer focus was extremely valuable in helping customers who were already “not happy”, and making sure they were heard and helped. Well done!!
Accomplishments

- **HSC M365 Go Live – Status COMPLETE**
  - Continued running Archives (items 2 years and older) migrations until two weeks prior to cutover and stopped at 90% to allow enough time to sync up current mail/calendar items.
  - Completed multiple incremental synchronizations of Active user mailboxes, including mail/calendar items, permissions, shared and resource mailboxes, contacts, and distribution groups prior to the cut over
  - Completed final version of cutover task list working with NetSec, Tier 2, and Systems teams.
  - The tasks for Go Live were straightforward and were completed within allotted time. There was additional clean up tasks afterward, but no issues and mail flow into Online Exchange through Proofpoint worked flawlessly.

- **Post Cut Over tasks and status**
  - We immediately began another round of incremental syncs against all user mailboxes to “catch up” the incoming mail between the last round of syncs and the cutover time. These completed in less than 24 hours.
  - Most of the support calls initially were around access to the environment and configuring the Outlook desktop client app. Later calls began to identify missing mail and calendar items which was expected to some extent.

- **Next Steps**
  - Continue running syncs to identify and resolve errors in data migration.
  - Run targeted syncs against individual mailboxes as necessary
  - Complete Archive data migrations
  - Work with ISO to implement security controls and multi-factor authentication (MFA)
  - Biweekly *M365 Migration Status Update* meeting with key Stakeholders continued
    - Future agenda will transition to GWIM replacement and other applications focus as well as MFA and overall Security hardening of the environment.

In-Progress

- Continue with post cutover migrations to get all data out of old exchange
- Continued work with vendor for replacement for Commvault Backup and Restore system and Ransomware protection.
  - 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
  - Characterized the enterprise data sets for capacity and structure
- Reviewing quotes for subscription
  - Solution transitions from periodic capital expenditures to ongoing operations costs – subscription based services.
- Continued work with Microsoft and third party vendor on completing Movere cloud cost analysis tool

**Metrics**

- **System Availability**
  - Impacts during Nessus scanning continued during scheduled scans on February 5\(^{th}\).
  - Worked with Networks and Nutanix Engineering to implement best practices for network configuration
    - No change during planned test on Feb. 19\(^{th}\). Impacts still occurred, but Systems, NetSec and Project ECHO IT were monitoring and shut down scans prior to impact.
    - Delayed March 5 scheduled scans until after O365 Go Live when we have opportunity to continue troubleshooting and RCA.

**Recognition**

- Bob Gagnon for nearly non-stop migration effort leading up to Go Live for O365
- Judson Carter for handling virtually all configuration and administration tasks in Office 365 and Azure
- Aaron Douglas for his efforts within Sailpoint and O365 provisioning as well as building the O365 Outlook client configurator tool
- Scott Hanson for his insights, knowledge, and efforts in planning the mail redirection from on premise to O365
INFORMATION SECURITY
MIKE MEYER

Accomplishments

<table>
<thead>
<tr>
<th>ACTION</th>
<th>IMPACT</th>
</tr>
</thead>
</table>
| Maintained very low vulnerabilities on public-facing devices and websites, especially for criticals and highs | Criticals – Continues at 0  
Highs - 0 (Decreased from 1)  
Medium 135 (Increased from 127) |
| Supported 365 deployment and related security reviews and research. | All hands were focused on Microsoft 365 in Feb, which deployed as scheduled 28 Feb 2021. Huge win for the organization. |
| All ISO staff manned the “365 Zoom Support Room” | This provided a nice “high touch” approach to customer service during the initial days of 365 support, and was a great team-building exercise with IT staff and managers from HSC CIO, UH and other units to work together. |

PERIMETER VULNERABILITIES – 1 FEB 2021

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>Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)</td>
<td>APR 2021 (Re-baselined from JAN 2021)</td>
<td>Green</td>
<td>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 Policy Manager. These tactical and strategic efforts will run in</td>
</tr>
</tbody>
</table>
We will collaborate through the Joint Network and Information System (JNIS) team (NetSec, UH Cyber, ISO) to accomplish these goals for the entire enterprise.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Due Date</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve configuration management (Tom/Michael Schalip)</td>
<td>JUN 2021 (re-baselined)</td>
<td>Green</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>
</tr>
<tr>
<td>Baseline Security Configuration for Windows (Zander)</td>
<td>MAR 2021 (Phase 1)</td>
<td>Green</td>
<td>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.</td>
</tr>
<tr>
<td>Analyze selected departments to determine how to increase workstation patching, encryption, and Windows 7 reduction</td>
<td>APR 2021</td>
<td>Green</td>
<td>Review security options and settings to meet Microsoft and government best practices for “HIPAA compliance” when we transition to 365.</td>
</tr>
<tr>
<td>Conduct Microsoft 365 security review</td>
<td>MAR 2021</td>
<td>GREEN</td>
<td>Review security options and settings to meet Microsoft and government best practices for “HIPAA compliance” when we transition to 365.</td>
</tr>
<tr>
<td>Issue new HSC Remote access policy. (Mike)</td>
<td>SEP 2020</td>
<td>Purple</td>
<td>Deferred due to other priorities.</td>
</tr>
<tr>
<td>Root Cause Analysis (RCA) process improvement (Tom/Mike)</td>
<td>JAN 2021</td>
<td>Complete JAN 2021</td>
<td>Aaron developed RCA template for Cherwell. Reviewed first RCA in CAB.</td>
</tr>
<tr>
<td>Improve process for review of Data User Agreement (DUA) for research (Mike/Zander)</td>
<td>DEC 2020</td>
<td>Complete JAN 2021</td>
<td>Under Privacy Officer’s lead, stakeholders reviewed forms and processes to decrease turnaround time for DUA processing.</td>
</tr>
</tbody>
</table>
**METRICS**

<table>
<thead>
<tr>
<th>METRIC</th>
<th>NUMBER</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)</td>
<td>• 22 Data User Agreements/secure data transfer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 31 Software/Cloud App Purchases and Renewals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8 Vulnerability Scans</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 38 Other</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF CONFIGURATION ITEMS PROCESSED</td>
<td>• 10 Change Requests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 Root Cause Analysis (RCA)</td>
<td></td>
</tr>
<tr>
<td>SSL CERTIFICATES ISSUED OR RENEWED</td>
<td>• 7</td>
<td></td>
</tr>
<tr>
<td>PERIMETER VULNERABILITIES</td>
<td>• Criticals – 0 (Same as previous month)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Highs – 0 (Decreased from 1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Medium – 135 (Increased from 127)</td>
<td></td>
</tr>
</tbody>
</table>

**RECOGNITIONS**

I want to recognize Zander Pegues. He is essentially the “ISO Service Desk.” He handles the bulk of the never-ending requests for security reviews of IT purchases, DUAs and other customer requests. Unfortunately, sometimes cyber cannot approve a specific request. When that happens, Zander makes every effort to help find the customer a solution that does comply with HSC policies and best practices—very often successfully. At a minimum, he takes the time to explain the security concerns to the customer. I receive a steady stream of emails from customers expressing their thanks for Zander’s help. You just don’t see that very often in the security field.

Besides being the mainstay in processing customer requests and questions, Zander is a team player. When we tightened down rules on email attachments and links in response to an imminent threat in late 2020, Zander volunteered to assist UH Cyber and NetSec in processing hundreds of customer requests for manual email release. He played a key role in finding process improvements as a participant in the Privacy Officer’s DUA process improvement team, which will reduce approval time for research projects. Most recently, he volunteered to man the 365 “Zoom support,” where I personally observed his gift for dealing with frazzled customers and resolving their 365 problems.

Zander is doing a great job supporting the ISO and HSC enterprise at large.
TECHNOLOGY SUPPORT

RICK ADCOCK

Accomplishments

- Published the Windows 10 ver 20h2 GM Standard workstation image.
- Published installer package for Office 2019 in Software Center.
- Created teams, onedrive, and outlook config advertisement’s for Apple workstations.
- In place upgrade for older versions of Windows 10 1703, 1809, 1909 so workstations can be upgraded without being re-imaged.
- Built Windows outlook configuration tools for email transition.
- Added more exchange functions to the identity management system.
- Tasked Tier 2 with creating one-click for bitlocker encryption lockouts.
- Developed onsite signage for IT support for opening of the building.
- Transitioned UME to Mediasite storage for Zoom recordings. (new content only)
- Created pre go-live checklist for people to enter Microsoft 365 and configure items before go-live.
- Developed and tested Post go-Live instructions for changing outlook desktop clients and mobile device apps.

In-Progress

- Live Microsoft 365 Training through march
- 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
- Hiring an IT Support Technician 2 for the College of Pharmacy
- Preparing a workstation replacement and budget for Health Sciences Rio Rancho
- 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.
- Hiring committee formation and process for replacing 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.
Metrics

Workstation Encryption

<table>
<thead>
<tr>
<th>Date / Group</th>
<th>Global UnEncrypted</th>
<th>Global Encrypted</th>
<th>Global Total</th>
<th>% Encrypt</th>
<th>% Encrypt</th>
<th>Unencrypted</th>
<th>Encrypted</th>
<th>Unknown</th>
<th>Total</th>
<th>% encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-12-2021 HSC</td>
<td>7148</td>
<td>6263</td>
<td>13411</td>
<td>53.30%</td>
<td>53.30%</td>
<td>3203</td>
<td>928</td>
<td>447</td>
<td>4578</td>
<td>20.27%</td>
</tr>
<tr>
<td>1-22-2021 HSC</td>
<td>5856</td>
<td>7579</td>
<td>13435</td>
<td>43.59%</td>
<td>43.59%</td>
<td>2488</td>
<td>2076</td>
<td>289</td>
<td>4853</td>
<td>42.78%</td>
</tr>
<tr>
<td>2-15-2021 HSC</td>
<td>5455</td>
<td>7569</td>
<td>13024</td>
<td>41.88%</td>
<td>41.88%</td>
<td>2097</td>
<td>2222</td>
<td>392</td>
<td>4711</td>
<td>47.17%</td>
</tr>
<tr>
<td>2-15-2021 UNMH</td>
<td>5455</td>
<td>7569</td>
<td>13024</td>
<td>41.88%</td>
<td>41.88%</td>
<td>2171</td>
<td>5068</td>
<td>963</td>
<td>8202</td>
<td>61.79%</td>
</tr>
</tbody>
</table>

HSC-O365 Help emails for February 648 as of (2/26)

Help Desk Call Stats Month

Total calls received: 1,526

Abandon rate: 8.78%

Recognition

Bob Gagnon for working on the email migration project and keeping us to date on progress and the assistance in investigating things so we can formulate accurate troubleshooting and resolution guidelines.
UH IT NETWORK/NETSEC
CHARLIE WEAVER

Accomplishments

- Zayo / Internet edge migration completed
- Support for M365 cutover
- Multiple JNIS subteam activities in process (Incident Management, Vulnerability Management, etc.)
- Multiple access switch upgrades completed at UH & Cancer Center
- Cerner circuit failover testing completed
- Network outage management as required
- Phase 2 ProofPoint Phase III (URL Defense) deployed
- Operational budget development completed
- Wombat (ProofPoint) anti-phishing tool demonstration completed; recommendation to purchase. Obtaining additional quotes to meet GSA purchase requirements
- Network Tech interviews in process

In-Progress

- Multi Factor Authentication team formed with goal of solution recommendation
- Century Link MOE capacity upgrade planned
- UH & Cancer Center access switch replacements continue
- UH / BBRP distribution switch replacement in planning
- Hiring decision for Network Tech
- High-level 2021 project planning

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

Microsoft 365

Cyber Security

Network Redesign

IT Service Management

Governance/Policies

Business Resiliency

1. Transfer domains
2. Data migration
3. Test
4. Training & Support
5. Phishing program
6. Upgrade Internet

1. 6 KPIs
2. MFA M365
3. RCA process
4. Vulnerability Assess
5. Staff development
6. Single service portal

1. Requirements
2. Network architect
3. Plan & Execute
4. KPIs
5. Staff development
6. Single service portal

1. 4 KPIs Dashboard
3. Service Recovery
4. Remote sup. tool
5. NPS survey/phone#
6. Single service portal

1. Charter for EIGC
2. Policy Manager
3. Update policies
4. IT Website upgrade
5. NPS survey/phone#
6. Single service portal

- - -
1) Communicate the **Vision** to your team 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, 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 **outsource 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 Adoption and Governance: IT Lead, Ray Avila