JUNE UNIT REPORTS

APPLICATIONS-RAY AVILA
SYSTEMS-PHIL MARQUEZ
SECURITY-MIKE MEYER
TECHNOLOGY SUPPORT-RICK ADCOCK
UH IT NETWORK/NETSEC-CHARLIE WEAVER

HSC 2021 VISION
Accomplishments

- Suspended HSC Attestation application
- Facilitated Trinetix data loads
- Launched new Learning Central courses
- Added Moodle storage space
- Provided course development support to HSC Moodle and Learning Central
- Launched IPE Honors dashboard
- Loaded faculty promotions for OFACD
- Provided various data requests
- Imported and processed student and faculty information to various systems supporting SOM
- Continued SailPoint administration training
- Developed/presented Knowledge Hub in SPO

In-Progress

<table>
<thead>
<tr>
<th>Projects in flight</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint Online / M365 transition – Active</td>
<td>3/1/2022</td>
</tr>
<tr>
<td>Faculty Directory Implementation</td>
<td>8/20/2021</td>
</tr>
</tbody>
</table>

Metrics

a. SP2010 EOL activity tracking:
   - Total sites: 73
   - Site Owner awaiting engagement – 53
   - Site Owner engaged/awaiting feedback – 8
   - Migration to SPO in process – 3
   - Migration to alternative platform in process – 1
   - Requiring vendor assistance – 0
   - Marked for deletion/abandonment: 8
Site Owner engagement status

- Site Owner awaiting engagement
- Migration to SPO in process
- Requiring vendor assistance
- Site Owner engaged/feedback pending
- Migration to alternative platform in process
- Marked for deletion/abandonment
Accomplishments

- Separated Employee Mail Migration
  - Brought the OnPrem Exchange environment back online after security event.
    - Brought up on premise domain controller (UH-XCHDC1) in Exchange environment isolated from Main Campus and the rest of HSC. Patched and installed Carbon Black.
    - Confirmed HSC.AD.UNM.EDU domain was back to functioning properly.
  - Updated all the AvePoint FLY servers with security patches and new version of FLY migration software. Successfully tested all connections from FLY to Exchange OnPrem and Exchange Online.
  - Created all TermedMailbox migration job mapping CSVs.
  - Created\Ran successful test migration jobs.
  - Kicked off the TermedMailbox production migration on 6/29 with 30 day window to complete.

- Azure/M365
  - Created Enterprise apps for Citrix test and Citrix-Prod to allow for SAML authentication
  - Creation of PhishAlarm integrated app to enable pushing of add-in to Outlook/OWA client.

- Datacenter
  - Removal of old DC hardware, installation of new.
  - Installation of NMTR file server and PowerVault

In-Progress

- Separated Employee Mail Migration
  - New versions of FLY software migrating data much faster than previous migration project. Expect completion of project within 30 day window with no issues.
- Continued supporting security efforts across HSC CIO supported servers and storage.
- Continued implementation of Metallic Cloud Backup across HSC servers.
- Continued support for MFA testing on CAG.
- Continued implementation of Metallic Cloud Backup across HSC managed servers and storage.
  - Outstanding items include:
    - Issues with a handful of Windows servers being worked.
    - Most Linux servers pending technical services engagement with Metallic engineer.
    - Issues with size of Dell NAS backup. Still in progress.

Metrics

- System Availability
  - Exchange environment completely down, but no longer in daily use for active email.
    - Impact to IPRA and Legal search capabilities for separated (not yet migrated) employees’ email – unable to complete searches against TermedMailboxes until Exchange environment came back on line.
Recognition

- Judson Carter and Bob Gagnon for bringing up a UH-owned domain controller in the Exchange environment and ensuring it was healthy and secure for the migration effort.
- Jason Barnes for his efforts to implement Metallic Cloud Backup.
# Accomplishments

<table>
<thead>
<tr>
<th>ACTION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSC CIO approved ISO re-assignment request. Michael Schalip is now formally attached to the ISO as Manager, Security Operations.</td>
<td>Mr. Schalip will now be even more proactive and visible in working within HSC CIO and with Health System counterparts to ensure that security operations are optimized and consistent.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: Most ISO resources focused on incident response in June.</td>
<td>Protect our data and network.</td>
</tr>
<tr>
<td>Continued to maintain very low vulnerabilities on public-facing devices and websites, especially for criticals and highs. The two highs in last month’s report are resolved.</td>
<td>Criticals – Continue at 0 Highs – Continue at 0 Medium – 130 (Decreased from 134)</td>
</tr>
<tr>
<td>Participated in data calls and discussions concerning renewal of our cyber breach insurance.</td>
<td>Cyber insurance needed to reduce potential liabilities.</td>
</tr>
<tr>
<td>Briefed senior leadership and provided steps needed now to reduce risk of similar incidents.</td>
<td>Leadership directed an acceleration of multi-factor authentication (MFA) for M365 and CAG and authorized funding for Endpoint Detection and Response (EDR).</td>
</tr>
<tr>
<td>Worked closely with both HSC CIO and UH Cyber Security elements to improve McAfee anti-virus (A/V) penetration on endpoints and improve performance on the server side.</td>
<td>Increasing A/V penetration and performance reduces risk of attacks.</td>
</tr>
</tbody>
</table>

## PERIMETER VULNERABILITIES

- **0 Critical (0/20)**
- **130 Medium (130/20)**
- **18 Low (18/20)**

99.6% Protected

### Prevented Malware

- **Known Malware**: 233
- **Suspect Malware**: 1
- **Non-Malware**: 1,044
- **PUPs**: 0

Total: 1,278
<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>Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN</td>
<td>JUL 2021</td>
<td>Red</td>
<td>Project is behind because we decided to implement on CAG first, but they are encountering technical challenges. As of 9 Jul, we decided to begin migration on M365 first, going by depts, and beginning 15 Jul 2021</td>
</tr>
<tr>
<td>Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)</td>
<td>Red 2021 – Brief ITAC, ECC, and EIGC so that policy and plan can be approved by core.</td>
<td>Red</td>
<td>Information Security Officer was not able to action the next steps in June due to incident response. Draft policy and strategy are 95% complete. NEXT STEPS: Provide draft of VM Strategy and policy to UH and HSC CIO. ITSC briefed. Brief ITAC and ECC in May, then submit Core review via PAW.</td>
</tr>
<tr>
<td>Improve configuration management (Tom)</td>
<td>JUN 2021 (re-baselined)</td>
<td>Yellow</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. <strong>NOTE:</strong> This will probably need to be re-baselined. It is a more complex objective than originally thought.</td>
</tr>
<tr>
<td>Cyber Security Strategic Plan (Mike)</td>
<td>FEB 2021 (2021 Goals)</td>
<td>Complete*</td>
<td>Brief 2021 strategic objectives. Develop long-term plan to improve cyber posture. <strong>Note:</strong> ISO deferred work on this milestone due to incident response.</td>
</tr>
<tr>
<td></td>
<td>AUG 2021 (2022+ Goals) (re-baselined from APR then again JUL)</td>
<td>Yellow</td>
<td></td>
</tr>
<tr>
<td>Conduct Microsoft 365 security review</td>
<td>MAR 2021</td>
<td>Complete Blue</td>
<td>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.</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>Task</td>
<td>Due Date</td>
<td>Status</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)</td>
<td>APR 2021</td>
<td>Complete</td>
<td>APR 2021 (for completion of policy and plan drafts for formal review as new HSC “cascaded” policy)</td>
</tr>
<tr>
<td>Issue new HSC Remote access policy. (Mike)</td>
<td>SEP 2020</td>
<td>Purple</td>
<td>SEP 2020 Deferred due to other priorities.</td>
</tr>
<tr>
<td>METRIC</td>
<td>NUMBER</td>
<td>NOTES</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF REQUESTS FOR SECURITY REVIEW THIS MONTH (ZANDER)</td>
<td></td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF CONFIGURATION ITEMS PROCESSED</td>
<td>13 Change Requests, three urgent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL CERTIFICATES ISSUED OR RENEWED</td>
<td>3 SSL certificates issued</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PERIMETER VULNERABILITIES</td>
<td>Criticals – 0 (Same as previous month)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highs – 0 (Same as previous month)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium – 130 (Decreased from 134)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recognition**

Marcia Sletten for her support to the Information Security Office during and following the incident. She has written multiple communications for topics like MFA, has facilitated and led meetings, and helped fast-track critical purchase requests such as the Endpoint Detection and Response (EDR) purchase. Marcia is not involved with the technical or operational aspects of information security, but her ability to make the system work fast when necessary was critical in our rapid implementation of Carbon Black EDR.

I just really appreciate that Marcia, like the other managers in CIO, are always willing to help whenever and when needed.
Accomplishments

- Updated SailPoint to 8.1p3 to allow more Microsoft Exchange data and coupling.
- Scripted access control for Citrix for users who have changed their password post 6/13/21.
- Wrote “Termed Maker scripts” for systems to populate old mailbox’s for migration.
- Tier 2 provided phone and desktop support in lieu of Tier 1 techs.
- Started work on re-architecting the HELP.HSC scheduling servers.
- Update OSX scripts to have more fail safe and easy flow.
- Updated OSX reporter for FVE to report more dynamically, due to DC changes.
- Hired and on-boarded two IT Support Tech 1 positions.

In-Progress

- NMTR Move to the Health domain.
- Interviewing for two IT Support Tech 2 positions for FY22.
- Creating a unified IT support model for the Rio Rancho campus.
- Continued support of the GEER grant.
- Resolving the workstation issues with McAfee and Carbon Black.
- Created an SCCM task sequence that uninstalls old versions of ENS and upgrade them through McAfee ENS 10.7 (1,743 workstations targeted).
- Developing a full return to the office plan.
- Multifactor Authentication deployment.
- Re-organization of the 317 offices to accommodate additional personnel.

Metrics

Tickets last quarter

![Tickets Per Day last quarter graph]

Tickets last year

![Tickets Per Day last year graph]
Recognition

Frank Roybal and his IT staff at Project Echo. We work closely with all of the departmental IT staff at the HSC. Project Echo IT staff who send us requests are articulate, accurate, and provide all of the necessary information we need to process their request in a timely manner and efficient manner. We appreciate that.
Accomplishments

- Most of the past month has been devoted to incident management & response.
- Multiple JNIS sub-team activities in flight (Incident Management, Vulnerability Management, etc.).
- UH distribution layer switches successfully replaced.
- HSC distribution layer switch configurations loaded and upgrades being scheduled.
- UH outside facility/building EOL access switch replacements beginning.
- Century Link MOE capacity upgrade completed.

In-Progress

- Century Link MOE capacity upgrade planning in process.
- CAG MFA integration experiencing technical difficulties; M365 rollout commencing.
- Outside facility access switch replacements commencing.
- FY22 equipment purchases beginning due to six+ month supply chain related lead-times.
- Beginning Optiv Managed Services Engagement.

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** 1\textsuperscript{st} year of a 5-year transformation journey.
18-Month Strategic Roadmap

<table>
<thead>
<tr>
<th>Year</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUL</td>
<td>AUG</td>
<td>SEPT</td>
</tr>
<tr>
<td>Microsoft 365</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Redesign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Service Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance/Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Resiliency</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Microsoft 365**
  - Cloud strategy
- **Cyber Security**
  - 1. Transfer domains
  - 2. Data migration
  - 3. Test
  - 4. Training & Support
  - 5. Phishing program
  - 6. Upgrade Internet
- **Network Redesign**
  - 1. Requirements
  - 2. Network architect
  - 3. Plan & Execute
  - 4. KPIs
  - 5. Staff development
  - 6. Update policies
- **IT Service Management**
  - 1. 4 KPIs Dashboard
  - 2. Network architect
  - 3. Plan & Execute
  - 4. KPIs
  - 5. Staff development
  - 6. Update policies
- **Governance/Policies**
  - 1. Charter for EIGC
  - 2. Policy Manager
  - 3. Update policies
  - 4. Remote sup. tool
- **Business Resiliency**
  - 1. Cloud strategy
  - 2. Backup/Recovery
  - 3. Web Hosting
1) Communicate the **Vision** to your team want to play in the big games.

2) Create the **Roadmap** to where you want remember to celebrate wins along the jo

3) Establish **Metrics** to guide and light the 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 Adaption and Governance: IT Lead, Ray Avila