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

APPLICATIONS

RAY AVILA

Accomplishments

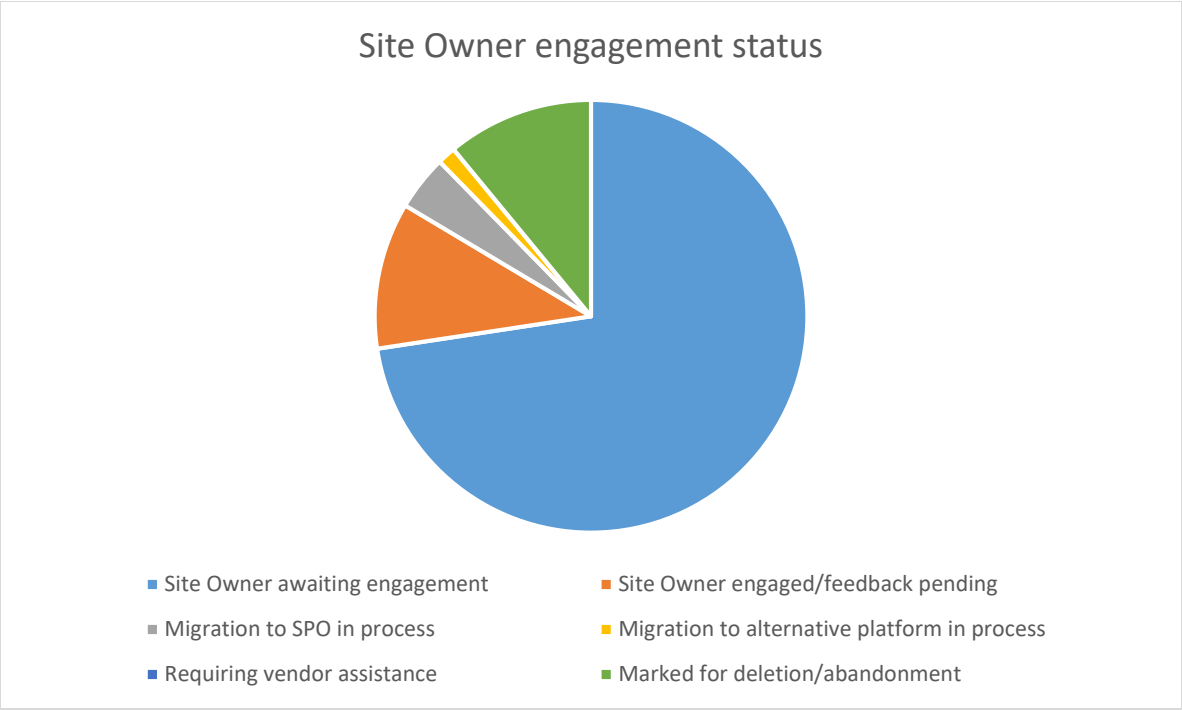
- Suspended HSC Attestation application
- Facilitated Trinetix data loads
- Launched new Learning Central courses
- Added Moodle storage space
- Provided course development support to HSC Moodle and Learning Central
- Launched IPE Honors dashboard
- Loaded faculty promotions for OFACD
- Provided various 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

Projects in flight	Status
SharePoint Online / M365 transition – Active	3/1/2022
Faculty Directory Implementation	8/20/2021

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

SYSTEMS

PHIL MARQUEZ

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

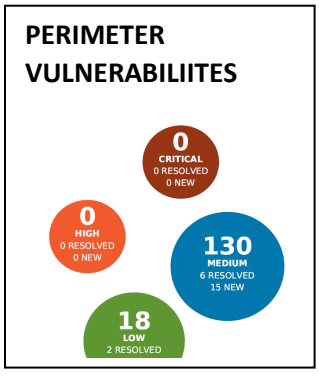
- Judson Carter and Bob Gagnon for bringing up a UH-owned domain controller in the Exchange environment and ensuring it was healthy and secure for the migration effort.
- Jason Barnes for his efforts to implement Metallic Cloud Backup.

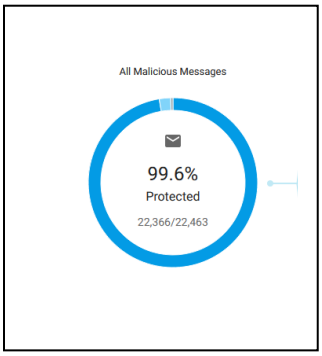
INFORMATION SECURITY

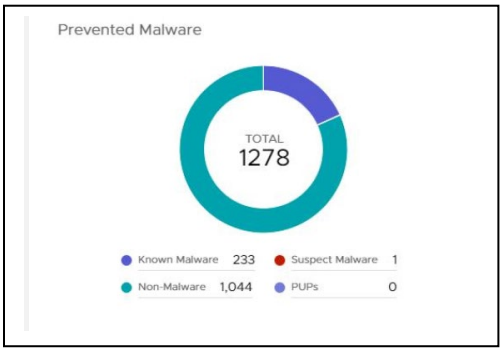
MIKE MEYER

Accomplishments

ACTION	IMPACT
HSC CIO approved ISO re-assignment request. Michael Schalip is now formally attached to the ISO as Manager, Security Operations.	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.
NOTE: Most ISO resources focused on incident response in June.	Protect our data and network.
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.	Criticals – Continue at 0 Highs – Continue at 0 Medium – 130 (Decreased from 134)
Participated in data calls and discussions concerning renewal of our cyber breach insurance.	Cyber insurance needed to reduce potential liabilities.
Briefed senior leadership and provided steps needed now to reduce risk of similar incidents.	Leadership directed an acceleration of multi-factor authentication (MFA) for M365 and CAG and authorized funding for Endpoint Detection and Response (EDR).
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.	Increasing A/V penetration and performance reduces risk of attacks.







In-Progress

PROJECT/ACTIVITY	PLANNED COMPLETION DATE	STATUS (Red, Yellow, Green)	NOTES
Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN	JUL 2021	Red	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
Vulnerability management – Develop mature process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)	Red 2021 – Brief ITAC, ECC, and EIGC so that policy and plan can be approved by core.	Red	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.
Improve configuration management (Tom)	JUN 2021 (re-baselined)	Yellow	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. **NOTE**: This will probably need to be re-baselined. It is a more complex objective than originally thought.
Cyber Security Strategic Plan (Mike)	FEB 2021 (2021 Goals)	Complete*	Brief 2021 strategic objectives. Develop long-term plan to improve cyber posture. **Note**: ISO deferred work on this milestone due to incident response.
	AUG 2021 (2022+ Goals) (re-baselined from APR then again JUL)	Yellow	
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.
Root Cause Analysis (RCA) process improvement (Tom/Mike)	JAN 2021	Complete JAN 2021	Aaron developed RCA template for Cherwell. Reviewed first RCA in CAB.

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)	Complete APR 2021	
Baseline Security Configuration for Windows (Zander)	MAR 2021 (Phase 1)	Complete	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.
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)	Complete Blue	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.
Baseline Security Configuration for Windows (Zander)	MAR 2021 (Phase 1)	Complete	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.
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 THIS MONTH (ZANDER)		Not available
NUMBER OF CONFIGURATION ITEMS PROCESSED	• 13 Change Requests, three urgent	
SSL CERTIFICATES ISSUED OR RENEWED	• 3 SSL certificates issued	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 0 (Same as previous month) • Medium – 130 (Decreased from 134)	

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.

TECHNOLOGY SUPPORT

RICK ADCOCK

Accomplishments

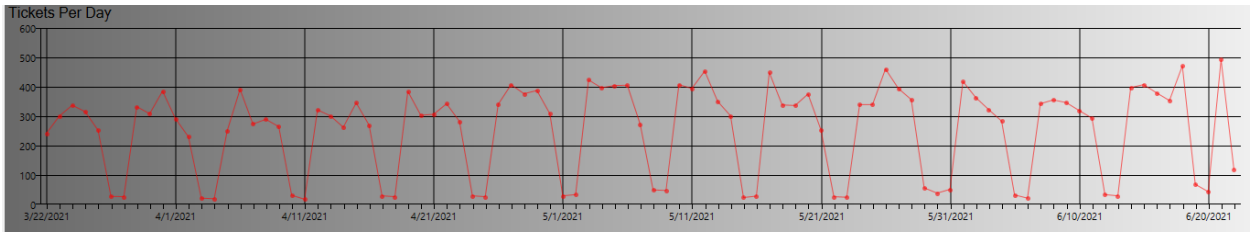
- Updated SailPoint to 8.1p3 to allow more Microsoft Exchange data and coupling.
- Scripted access control for Citrix for users who have changed their password post 6/13/21.
- Wrote “Termed Maker scripts” for systems to populate old mailbox’s for migration.
- Tier 2 provided phone and desktop support 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

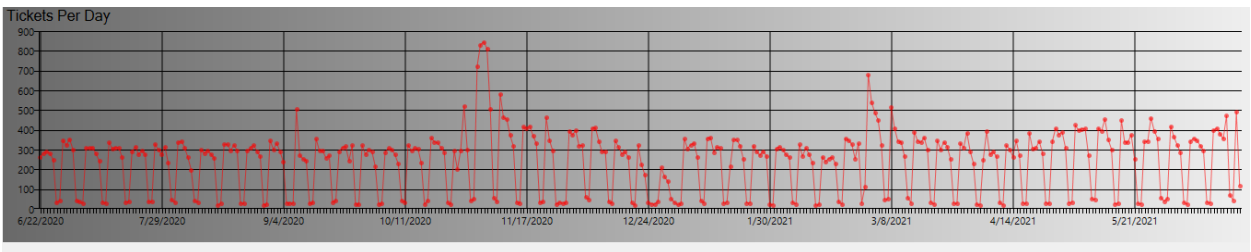
- NMTR Move to the Health domain.
- Interviewing for two IT Support Tech 2 positions for FY22.
- Creating a unified IT support model for the Rio Rancho campus.
- Continued support of the GEER grant.
- Resolving the workstation issues with McAfee and Carbon Black.
- Created an SCCM task sequence that 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 last year



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.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

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