HEALTH
SCIENCES
CHIEF INFORMATION
OFFICE

JULY 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

- Created new course materials and tutorials for Moodle and Learning Central
- Provided curriculum support for Moodle and Learning Central
- Facilitated Zoom support sessions for MultiFactor Authentication (MFA)
- Successfully tested PolicyManager attestation and newly created LDAP rules
- Continued SailPoint administrator training

In-Progress

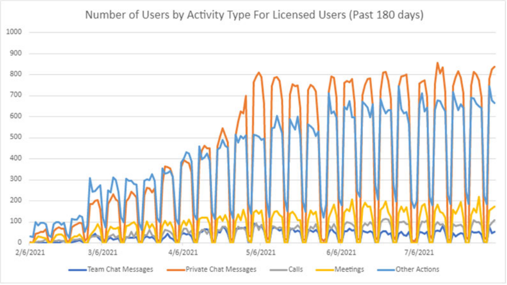
Projects in flight	Status
SharePoint Online/M365 transition – Active	3/1/2022
Faculty Directory implementation	8/20/2021

Metrics

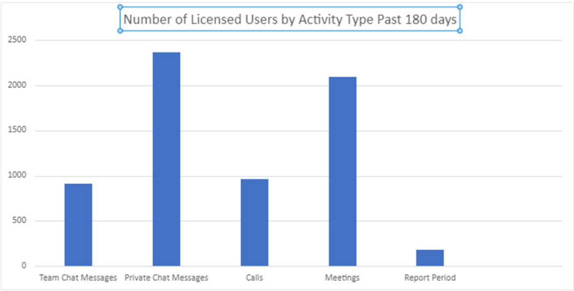
- SharePoint2010 End-of-Life (EOL) activity tracking:
  Total sites: 73
  Site Owner awaiting engagement - 49
  Site Owner engaged/awaiting feedback - 8
  Migration to SharePoint On-line (SPO) in process - 7
  Migration to alternative platform in process - 1
  Requiring vendor assistance - 0
  Marked for deletion/abandonment - 11

- M365 usage information:

Teams Activity:

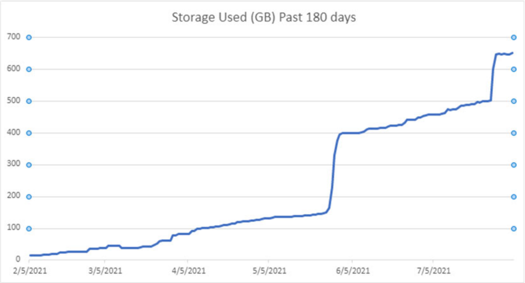


Teams usage:

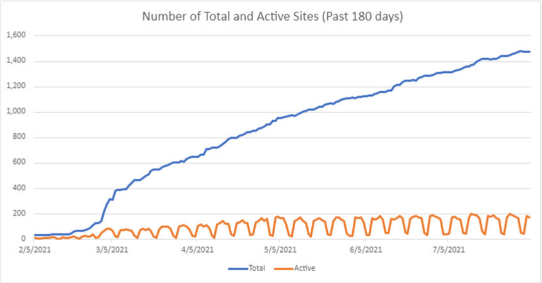


.

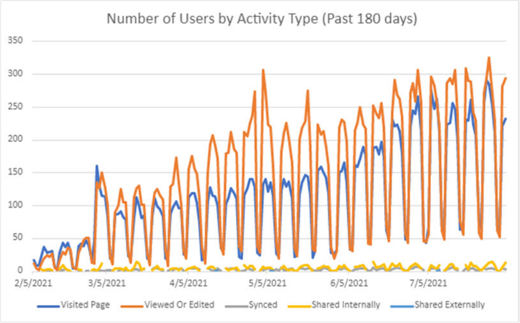
SharePoint Online Storage Use:



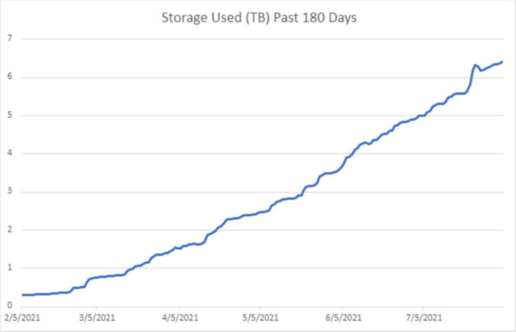
SharePoint Online Total and Active Sites:



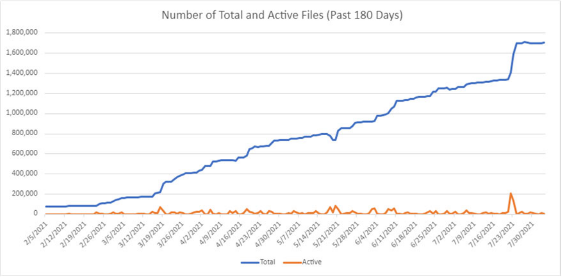
SharePoint Online users by activity:



OneDrive Storage use:



OneDrive File Count:



SYSTEMS

PHIL MARQUEZ

Accomplishments

- Exchange Mail Migration to M365 complete
  - The migration of separated employee mailbox data was completed closing out the email migration project.
  - The old on-premise Exchange environment has been turned over to UH Systems team to decommission the hardware.
- Azure/M365
  - Configured MFA to be functional across the organization as groups continue to be added
  - Configured new PhishAlarm button to appear in Desktop and web-based Outlook clients
- Metallic cloud backup implementation fully configured and almost complete for protected servers.
  - Initial phase was to migrate Commvault backups to Metallic
  - Next phase is to identify areas not yet being backed up
  - Future phase is to look at M365 backup protection

In-Progress

- Continued supporting security efforts across HSC CIO supported servers and storage
- Continued implementation of Metallic Cloud backup across HSC managed servers and storage
  - Dell NAS initial full backup still in progress. Initial full backups take a lot of time.
- Investigating refresh of on-site storage hardware

Metrics

- No System Downtime

Recognition

- Marcia Sletten for her efforts to support office space improvements and telecommuting work plans.
- Antoinette Martinez for her purchasing and finance support in budget preparation, reminders of upcoming recurring renewals, processing large purchases and tracking ongoing budget status.

INFORMATION SECURITY

MIKE MEYER

Accomplishments

ACTION	IMPACT
Completed lessons learned from incident, including top 20 security enhancements. Briefings began.	Prioritized roadmap for enhancing security to reduce risk from our biggest threat – ransomware.
Carbon Black endpoint detection and response extended for three years with managed services.	We now have one of the key controls that security experts and insurers recommend. Managed services means that we have a company monitoring activity and alerting us 24x7 when immediate action is required.
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 - Continues at 0 Highs - Continues at 0 Medium - 119 (Decreased from 130)
Deployment of multi-factor authentication on Microsoft 365 is underway and about 50% complete.	99.9% prevention of user credential theft, thus a significant reduction in ransomware risk.

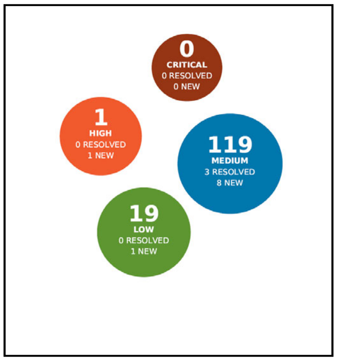
In-Progress

PROJECT/ACTIVITY	PLANNED COMPLETION DATE	STATUS (Red, Yellow, Green)	NOTES
Ransomware Playbook for incident response	SEP 2021	Green	Goal is to improve our response to any future ransomware attempts.
Turn "Top 20 Security Enhancements" into roadmap	OCT 2021	Green	
Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN	JUL 2021	Red	365 MFA rollout approximately 50% complete, with completion expected NLT 30 Aug. CAG MFA continues to encounter technical problems.
Vulnerability management – Develop mature	Red 2021 – Brief ITAC, ECC, and EIGC so that	Yellow	ISO briefed ITAC.

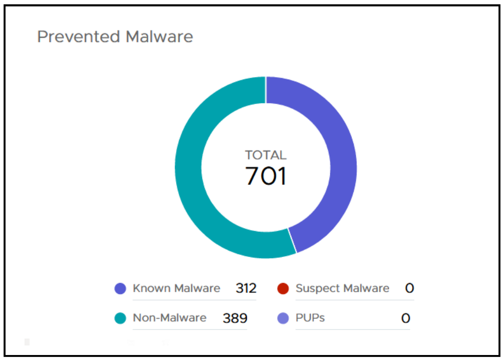
process to identify and track perimeter vulnerabilities and their mitigations (Michael Schalip/Zander)	policy and plan can be approved by core.	🟨	
Cyber Security Strategic Plan (Mike)	FEB 2021 (2021 Goals)	Complete*	Brief 2021 strategic objectives. Develop long-term plan to improve cyber posture. **Note**: ISO deferred work on this milestone due to incident response.
	AUG 2021 (2022+ Goals) (re-baselined from APR then again JUL)	Yellow	

METRICS (Last 30 Days)

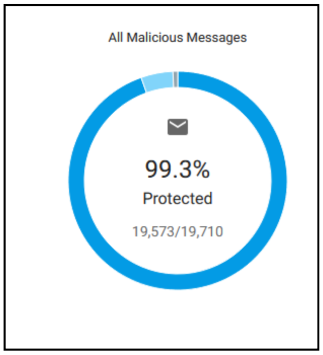
Perimeter Vulnerabilities



Malware Prevented by EDR



Malicious Messages Blocked



METRIC	NUMBER	NOTES
Malicious inbound email messages blocked	19,710	
Malware stopped by Carbon Black endpoint detection and response (EDR)	701	
Data Loss Prevention (DLP) – Outbound emails blocked for PHI	• **287**	Proofpoint is our email filtering application

METRIC	NUMBER	NOTES
NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)	• 19 Data User Agreements/secure data transfer requests • 24 Software/Cloud App Purchases and Renewals • 5 Vulnerability Scans • 38 Other	
CHANGE REQUESTS	• 10 Change Request	
SSL CERTIFICATES ISSUED OR RENEWED	• 1 SSL certificates issued	
PERIMETER VULNERABITIES	• Criticals – 0 (Same as previous month) • Highs – 0 (Same as previous month) • Medium – 119 (Decreased from 130)	

Recognition

Mr. Michael Schalip must be recognized for his relentless efforts in managing and leading the deployment of Carbon Black EDR and managed services, which went live on 4 Aug 2021. His efforts not only to manage the transition but to communicate widely among stakeholders directly contributed to the resounding success of this effort and the new protection against ransomware that it provides. Mr. Schalip has found a home in the ISO and we are glad to have him.

TECHNOLOGY SUPPORT

RICK ADCOCK

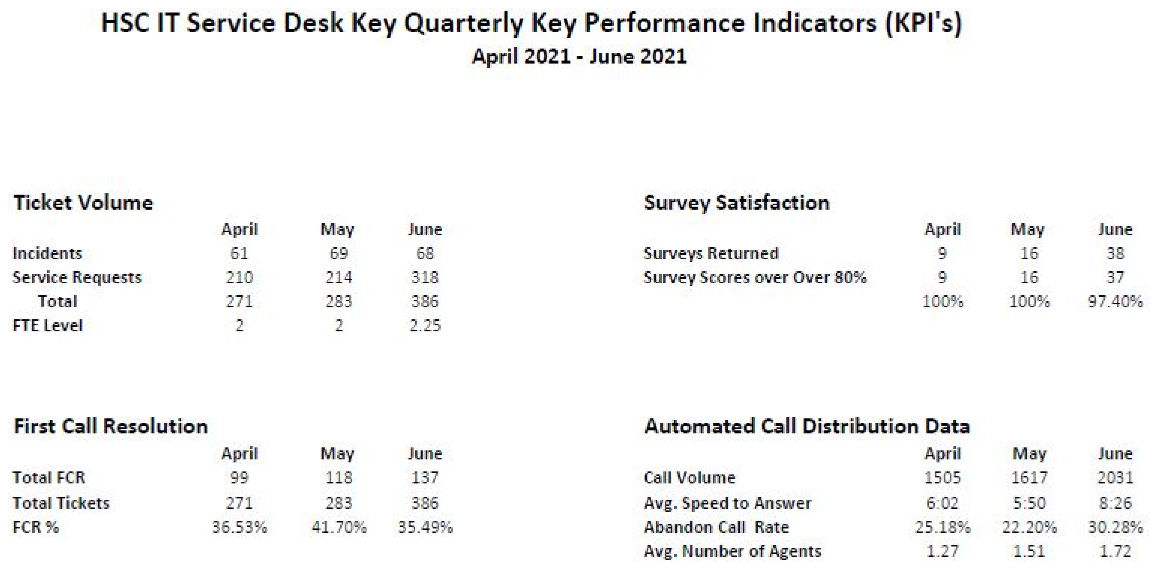
Accomplishments

- Finished interviews for IT Support Tech 2 position
- Patched SailPoint to version 8.1p3, and setup Azure Active Directory synchronization
- Setup MFA groups and entitlements
- Built and pushed Carbon Black to OSX Management
- Built Munki reporting dashboard
- Data analysis for Carbon Black bypass devices
- Provided Training for New IT Service Desk staff
- Data Analysis for McAfee version issues

In-Progress

- Multifactor Authentication Deployment
- NMTR Move to the Health domain
- Continued support of the GEER grant
- Re-organization of HSLIC room 317 offices to accommodate additional personnel
- Defining processes for new endpoint security monitoring
- Obtaining job skill codes in the Banner feed to correctly assign Microsoft licenses
- Deploying workstation hardening group policy

Metrics



HSC IT Service Desk Key Quarterly Key Performance Indicators (KPI's)

April 2021 - June 2021

Ticket Volume

	April	May	June
Incidents	61	69	68
Service Requests	210	214	318
Total	271	283	386
FTE Level	2	2	2.25

Survey Satisfaction

	April	May	June
Surveys Returned	9	16	38
Survey Scores over Over 80%	9	16	37
	100%	100%	97.40%

First Call Resolution

	April	May	June
Total FCR	99	118	137
Total Tickets	271	283	386
FCR %	36.53%	41.70%	35.49%

Automated Call Distribution Data

	April	May	June
Call Volume	1505	1617	2031
Avg. Speed to Answer	6:02	5:50	8:26
Abandon Call Rate	25.18%	22.20%	30.28%
Avg. Number of Agents	1.27	1.51	1.72

Recognition

Vernon Bell has a very strong work ethic. He is always here and on time and stays as long as needed. He is extremely productive, he moves from one task to the next and keeps going. He is someone that the faculty and staff can count on as well as his peers. Vernon has been on-site providing IT phone support for HSC faculty, staff, and students during the entire pandemic. Vernon is also an 18 year employee who has served in IT positions in OB/GYN, Pediatrics, Cancer Center, and the CIO office.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Most of the past month has been devoted to incident management & response
- **Network change freeze in place due to recent outages**
  - **Data Center network 7/13**
  - **HSSB Core switch 7/23**
  - **Root cause ascertained for both**
- Multiple JNIS sub team activities (Incident Management, Vulnerability Management, etc.) in flight
- UNM/Century Link fiber reroute project beginning

In-Progress

- Network Managed Service option being explored
- CAG MFA integration continuing to experience integration difficulties; 365 roll-out commencing
- Outside facility access switch replacements on hold
- UH distribution layer switch replacements on hold
- HSC distribution layer switch replacements on hold
- FY22 equipment purchases beginning due to six+ month supply chain related lead-times
- ANM Advanced Services engagement for data center network & overall network ‘get well’ plan in process

Metrics

Total Access Layer Switches (UNMH, HSC, Remote):	~700
Total Access Layer Switches replaced to date:	51
Access Layer Switch replacement % completion:	**~7%**
Total Distribution Layer Switches (UNMH, HSC):	41
Total Access Layer Switches replaced to date:	8
Distribution Layer Switch replacement % completion:	**~19%**

Recognition

- HSO ISO & Cyber Security team for outstanding teamwork

1) **Security** first, then everything follows.

2) **Cloudification** with an emphasize on storage, backup and recovery.

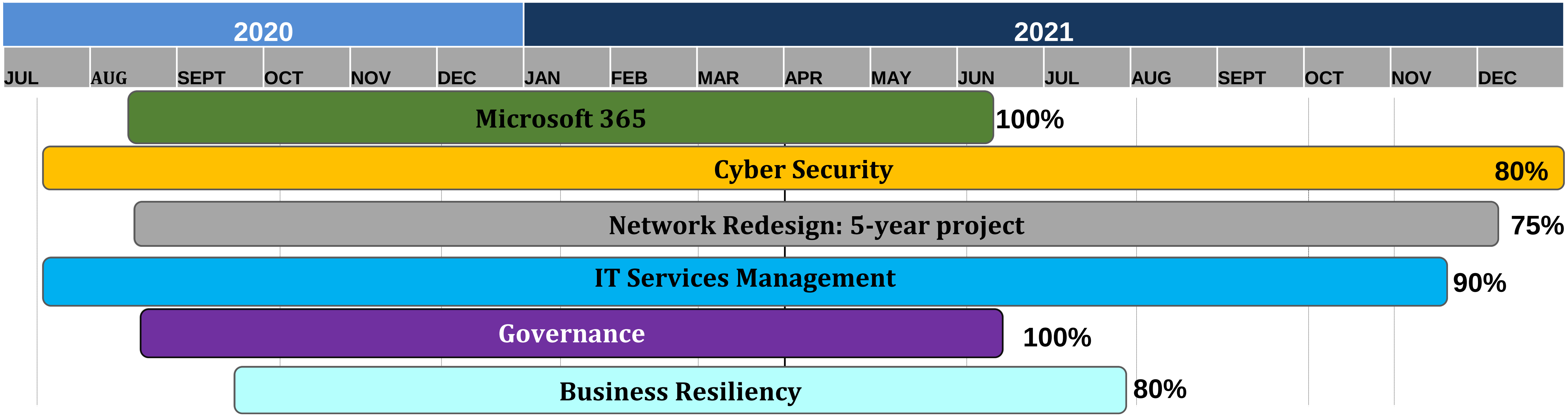
3) **Service Delivery** from our customers’ perspective.

4) **Collaboration** with Microsoft 365 adoption.

5) **Network Modernization** 1st year of a 5-year transformation journey.

18-Month Strategic Roadmap

Marquez	Meyer	Weaver	Adcock	Sletten	Marquez
Microsoft 365	**Cyber Security**	**Network Redesign**	**IT Service Management**	**Governance/Policies**	**Business Resiliency**
~~1. Transfer domains~~	~~1. 6 KPIs~~	~~1. Requirements~~	~~1. 4 KPIs Dashboard~~	~~1. Charter for EIGC~~	1. Storage upgrade
~~2. Data migration~~	2. Azure MFA	~~2. Network architect~~	~~2. Aging tickets Rpt~~.	~~2. Policy Manager~~	2. Backup/Recovery
~~3. Test~~	3. RCA process	3. Phase 1 of 3 in prog	~~3. Service Recovery~~	~~3. IT Website upgrade~~	
4. Training & Support	4. Vulnerability Assess	4. KPIs	~~4. Remote sup. tool~~		
5. ~~Archived Termed EE~~	5. Phishing program	5. Staff development	5. NPS survey		
	6. CMMC framework	6. ~~Upgrade Internet~~	6. Single service portal		


JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEPT
OCT
NOV
DEC
Microsoft 365
Cyber Security
Network Redesign: 5-year project
IT Services Management
Governance
Business Resiliency