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

<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

- 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:
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

<table>
<thead>
<tr>
<th>ACTION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed lessons learned from incident, including top 20 security enhancements. Briefings began.</td>
<td>Prioritized roadmap for enhancing security to reduce risk from our biggest threat – ransomware.</td>
</tr>
<tr>
<td>Carbon Black endpoint detection and response extended for three years with managed services.</td>
<td>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.</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 - Continues at 0 Highs - Continues at 0 Medium - 119 (Decreased from 130)</td>
</tr>
<tr>
<td>Deployment of multi-factor authentication on Microsoft 365 is underway and about 50% complete.</td>
<td>99.9% prevention of user credential theft, thus a significant reduction in ransomware risk.</td>
</tr>
</tbody>
</table>

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>Ransomware Playbook for incident response</td>
<td>SEP 2021</td>
<td>Green</td>
<td>Goal is to improve our response to any future ransomware attempts.</td>
</tr>
<tr>
<td>Turn “Top 20 Security Enhancements” into roadmap</td>
<td>OCT 2021</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Implement Microsoft Multi-Factor Authentication for M365, CAG and VPN</td>
<td>JUL 2021</td>
<td>Red</td>
<td>365 MFA rollout approximately 50% complete, with completion expected NLT 30 Aug. CAG MFA continues to encounter technical problems.</td>
</tr>
<tr>
<td>Vulnerability management – Develop mature</td>
<td>Red 2021 – Brief ITAC, ECC, and EIGC so that</td>
<td>Yellow</td>
<td>ISO briefed ITAC.</td>
</tr>
</tbody>
</table>
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.

**AUG 2021 (2022+ Goals)** (re-baselined from APR then again JUL)

**Yellow**

Note: ISO deferred work on this milestone due to incident response.

**METRICS (Last 30 Days)**

<table>
<thead>
<tr>
<th>Perimeter Vulnerabilities</th>
<th>Malware Prevented by EDR</th>
<th>Malicious Messages Blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prevented Malware</strong></td>
<td><strong>TOTAL 701</strong></td>
<td><strong>99.3% Protected</strong></td>
</tr>
<tr>
<td>1 Low Priority 36%</td>
<td>312 Known Malware</td>
<td>19,573/19,710</td>
</tr>
<tr>
<td>119 Medium Priority 34%</td>
<td>389 Non-Malware</td>
<td></td>
</tr>
<tr>
<td>19 High Priority 30%</td>
<td>701 Suspicious Malware</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>METRIC</th>
<th>NUMBER</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious inbound email messages blocked</td>
<td>19,710</td>
<td></td>
</tr>
<tr>
<td>Malware stopped by Carbon Black endpoint detection and response (EDR)</td>
<td>701</td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention (DLP) – Outbound emails blocked for PHI</td>
<td><strong>287</strong></td>
<td>Proofpoint is our email filtering application</td>
</tr>
<tr>
<td>METRIC</td>
<td>NUMBER</td>
<td>NOTES</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>NUMBER OF REQUESTS FOR SECURITY REVIEW REQUESTS THIS MONTH (ZANDER)</td>
<td>• 19 Data User Agreements/secure data transfer requests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 24 Software/Cloud App Purchases and Renewals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5 Vulnerability Scans</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 38 Other</td>
<td></td>
</tr>
<tr>
<td>CHANGE REQUESTS</td>
<td>• 10 Change Request</td>
<td></td>
</tr>
<tr>
<td>SSL CERTIFICATES ISSUED OR RENEWED</td>
<td>• 1 SSL certificates issued</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 (Same as previous month)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Medium – 119 (Decreased from 130)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Ticket Volume</th>
<th>April</th>
<th>May</th>
<th>June</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>61</td>
<td>69</td>
<td>68</td>
</tr>
<tr>
<td>Service Requests</td>
<td>210</td>
<td>214</td>
<td>316</td>
</tr>
<tr>
<td>Total</td>
<td>271</td>
<td>283</td>
<td>388</td>
</tr>
<tr>
<td>FTE Level</td>
<td>2</td>
<td>2</td>
<td>2.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Survey Satisfaction</th>
<th>April</th>
<th>May</th>
<th>June</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surveys Returned</td>
<td>9</td>
<td>16</td>
<td>38</td>
</tr>
<tr>
<td>Survey Scores over 80%</td>
<td>100%</td>
<td>100%</td>
<td>97.40%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First Call Resolution</th>
<th>April</th>
<th>May</th>
<th>June</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FCR</td>
<td>99</td>
<td>118</td>
<td>157</td>
</tr>
<tr>
<td>Total Tickets</td>
<td>271</td>
<td>283</td>
<td>388</td>
</tr>
<tr>
<td>FCR %</td>
<td>36.53%</td>
<td>41.70%</td>
<td>33.49%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automated Call Distribution Data</th>
<th>April</th>
<th>May</th>
<th>June</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Volume</td>
<td>1505</td>
<td>1617</td>
<td>2031</td>
</tr>
<tr>
<td>Avg. Speed to Answer</td>
<td>6.02</td>
<td>5.30</td>
<td>8.31</td>
</tr>
<tr>
<td>Abandon Call Rate</td>
<td>25.18%</td>
<td>22.72%</td>
<td>30.28%</td>
</tr>
<tr>
<td>Avg. Number of Agents</td>
<td>1.27</td>
<td>1.51</td>
<td>1.72</td>
</tr>
</tbody>
</table>
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.
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** 1\(^{st}\) year of a 5-year transformation journey.
18-Month Strategic Roadmap

**Microsoft 365**
- Transfer domains
- Data migration
- Test
- Training & Support
- Archived-Termed EE

**Cyber Security**
- 6 KPIs
- Azure MFA
- RCA process
- Vulnerability Assess
- Phishing program
- CMMC framework

**Network Redesign**
- Requirements
- Network architect
- Phase 1 of 3 in prog
- KPIs
- Staff development
- Upgrade Internet

**IT Service Management**
- 4 KPIs Dashboard
- Aging tickets Rpt.
- Service Recovery
- Remote sup. tool

**Governance/Policies**
- Charter for EIGC
- Policy Manager
- IT-Website upgrade

**Business Resiliency**
- Storage upgrade
- Backup/Recovery

---

**2020**

- **JUL:** Marquez
  - Microsoft 365
    - 100%
  - Cyber Security
    - 80%

- **AUG:** Meyer
  - Network Redesign: 5-year project
    - 75%

- **SEPT:** Adcock
  - IT Services Management
    - 90%

- **OCT:** Sletten
  - Governance
    - 100%

- **NOV:** Marquez
  - Business Resiliency
    - 80%

- **DEC:**
  - Microsoft 365
  - Cyber Security
  - Network Redesign: 5-year project
  - IT Services Management
  - Governance
  - Business Resiliency