IT Council Meeting Minutes 02/05/2024

Policy Update X-3.03

Klauda noted that he submitted the proposal to update policy X-3.03 to the Senate Executive Committee just after their January meeting, and they will review the proposal in their February meeting. Klauda looks forward to hearing from volunteers who wish to join the subcommittee that will work on this policy revision.

Working Group Updates

Klauda provided the Administrative Systems Working Group update in Julie Wright's absence. The working group met on Thursday 1/25/24 and covered the following topics:

Elevate - Update and a discussion on "go live" date - Chris Wilkins

Wilkins noted the recent success with the transition of two legacy time clock systems to 1 cloud based clock system that supported its first payroll process over the winter break.

Regarding the Elevate Student project, the Executive Steering Committee was finalized. The mainframe core code is 40 years old with student data. The platform has to have the HR/Payroll/Finance piece in place first and then they will move to the student interface. The Steering Group is a formal governance group that was charged last fall and they will make decisions on deployment. There will be more to report in the Spring after the Steering Committee gets acclimated and begins its work.

Go Live Date - Elevate - HCM/Finance

President Pines will make the ultimate decision based on the best time of year for the universal stakeholder groups. There was a root cause analysis done when the last Go Live date was put on hold and there were technical issues between the College Park campus payroll date and what was transmitted to the state system that processes payroll. Continued testing is ongoing and has been successful thus far.

KFS and PHR - With regards to accessing it via VPN, Persaud noted that, as of this February, IT finished with the upgrades. There is an RFP for a new ID and locking system as the magstripes are at end of life.

We are now beginning with the below process:

- Reprint all new IDs with legacy magstripe to translate across campus
- Once we hit critical mass, we stop producing cards with legacy magstripe
- Phase 2 - Student facing services that require cards
- Phase 3 - All academic and administrative buildings

- Persaud and others have been charged to lead a committee on AI. Persaud has asked for ideas and feedback on how AI be helpful to the campus community
    - IT has been working with graduate school and College of Education on a BOT that answers policy questions with AI

Persaud also reported that each month there is a Deputy CIO Big 10 meeting, and this past month, Michigan presented their AI solutions for students. For example, if a class presentation was in ELMS Canvas, and they had a question about that presentation, students can ask their BOT, and it would find the reference in the recorded class. What students appreciate is that basic questions can be answered by the BOT outside of class hours. Instructors noted that because of this, the student relationship and quality of learning has been enriched by the opportunity to have a higher level discussion.

Persaud provided the IT Infrastructure Working Group update for Augustus Sam. The working group met on 1/18/24 and covered the following topics:

- They spoke about defining policies and procedures for department lead initiatives procuring technology infrastructure (i.e: Distributed Antenna Systems, Telecommunications, CableTV)
- Hollingsworth discussed providing information to the CFO on major "big ticket" procurement initiatives which impact the overall campus budget
- Working group leadership will draft a document by 2/8 to be shared with the working group to outline the policies and procedures
- Creating SOP for onboarding new hardware and software to the campus network to assist with capacity planning, security, and performance,

Klauda provided the It Security Working Group update for Mary Shelly. The working group met on 1/24/24 and covered the following topics:

IT Security

- Sneeringer reviewed and there was a discussion on the interim standard IT-17 Incident Response
- Gridley discussed data inventory requirements
- Sneeringer reviewed and there was a discussion of a draft BYOD (Bring your own Device) standard with a focus on the circumstances that can compel an employee to produce a personal device for inspection
- Appropriate data classification level to ban from personal devices
- 3rd party software process update -- moving into ServiceNow then additional testing and training before a broader rollout
- Plan to review IT-5 and IT-14 this year
- Security Updates from Gerry re: DYS

Learning Technology (Chair Derek Richardson)

- No meeting in January. Next meeting is scheduled for Feb 7.

Research Technology (Chair, Abhinav Bhatele)

- No meeting in January. Next meeting is scheduled for Feb 12.

Campus Wide Incident Response - Jeff Hollingsworth

Hollingsworth reported that UMD's leadership has been working to continually improve their processes of reporting and managing campus incidents. As part of that effort, DIT has refined the processes of notifying key stakeholders when a major IT incident occurs. Hollingsworth noted that If an event meeting the general criteria below was occurring, anyone can call UMD's Office of Emergency Management and Business Continuity (OEMBC) at 301-226-2266 in addition to escalating within DIT. The OEMBC number is staffed 24 hours a day, including holidays and weekends. If someone is not sure if an incident rises to this level, you can call OEMBC and someone will help you determine if the situation is a campus-level incident. Notifying OEMBC does not replace notifying relevant personnel in DIT and other units but should be conducted at the same time as those notifications. Any call to OEMBC, even if further action is not taken, is shared with the Campus Incident Strategy Group for situational awareness.

General Criteria: Events meeting the threshold level are ones that cause the unplanned suspension of normal teaching, research, or administrative activities for hundreds to thousands of users (students, faculty, or staff). Planned outages that have been communicated ahead of time are not campus-level incidents.

Below are illustrative examples of campus-level IT incidents (other incidents with similar impact would also qualify as campus-level incidents):

Substantial network outage lasting 10 or more minutes (any time of day/weekend/holiday):

- The UMD campus phone system is down or no calls can be made to/from campus.
- The UMD wireless network is not working or a dozen people report that they can not connect. (Note: Since relatively few people report an outage, a dozen reports likely means more than a hundred people are impacted.)
- The wired network is down in an entire major academic building (e.g., ESJ), or it is down in two or more other buildings. A major academic building is one with 500 or more general purpose classroom seats. A list of such buildings is at the end of this memo.
- All networking connectivity between campus and critical cloud-hosted services (e.g., Google, AWS, Azure, Infrastructure, Workday, DUO) is lost.

Outage (service down or not reachable) of a critical campus-wide service lasting 10 or more minutes (any time of day/weekend/holiday):

- CAS/DUO (shared login) is down thus preventing login to many/most other systems.
- Google Workspace Suite (Gmail, Google Drive) is down.

- Zoom is down.
- ELMS-Canvas is down.

Note: Depending on the time of occurrence, outages of other systems may rise to campus-level incidents. For example a SIS/Testudo outage during the first week of class or KFS during fiscal closing. Determination if these types of impacts are campus-level incidents should be made by the CIO or their direct reports since declaring an incident here is not as time-critical as other systems on this list.

Cybersecurity events (any time of day/weekend/holiday):

Any event that meets the threshold of a "High Severity Incident" as defined by the Interim Standard for IT Security Incident Response (IT-17).

Indications of a cybersecurity incident (compromised system or ransomware) that has crossed from a single computer (or few computers) to one that is impacting more than a dozen computers (or more than two campus units). Due to the sensitivity of these types of events, notification to OEMBC should come from the DIT Security Operations Center (SOC), the CIO, or direct reports to the CIO. Should anyone suspect a cybersecurity incident, they should immediately contact the SOC (soc@umd.edu, 301-226-4225).

Cybersecurity/Incident + Operating Posture - Jeff Hollingsworth

Hollingsworth then presented on the topic of Cybersecurity incidents and the operating posture.

Problems

- Recent Cyber Security Events
  - Compromise of an administrative unit's Windows Sever
  - Compromise of multiple servers & clients in a research organization
  - Inability of DIT/President's Office to disable a terminated employee's laptop in a timely manner
- Varied and Unknown backup procedures across campus
- Servers in assorted campus locations
  - Varying quality of HVAC, Power, and Physical Security

Requirements

- Assurance that all devices on campus are:
  - patched in a timely manner to prevent exploitation.
  - backed up to permit recovery after a loss, disaster, or cyber event.
- Rapid deployment of security software (i.e. FireEye, VPN)
- Allow local units to administer machines with unique needs
- Allow waivers for backup requirement of select research data
  - Too large to practically backup
  - Replicated elsewhere in the world

Proposed Solution- Central Patching & Identity

- Require remote management tools on computers
  - Tools: Intune(Windows clients), MECM(Windows Servers) or Jamf(Mac) on all UMD owned Windows & MAC computers
  - Provides central (DIT) visibility/review of patching across campus
  - Allows unit IT to customize installed software and time patch deployment
  - In urgent situations, DIT can patch any/all computers as needed
  - Reduces efforts to update common software (VPN, FireEye, etc.)
  - Intune is already on 7,200 of 13,000 UMD windows client machines
  - Jamf is currently on a majority of Mac systems

- Retirement of locally operated identity servers (Active Directory & LDAP)
  - Already underway as part of network refresh
  - 5 of 13 units will be done by 3/1/24 (2 are done already)
  - Potentially require Rapid7 Insight on Linux systems

Richardson asked about the Intune system options when engaged. Hollingsworth noted that in almost all cases, there is a selected time option to reboot, but in the case that serious malware were circulating, you could engage the software immediately.

Bauman noted that, in regards to patches, he asked how a balance is being struck with flexibility for the end user. Hollingsworth shared that he has had experiences that were not user friendly and he is not creating that environment here. With 99% of computers associated with the University, the expectation is that a installation would be user friendly and that you would have the latest patched version for the update.

Bauman asked how personal devices would be handled in the future and Hollinsgworth noted that the IT Security Working Group is putting together a BYOD policy.

Proposed Solution: Authority to Operate (ATO) Model

- Units administering computers/servers/cloud services must:
  - Be registered with and approved by CIO or designee
  - Meet DIT established standards such as (final standards TBD):
    - Two IT staff on 24/7 on call for emergencies
    - Mandated security software installed on all systems
    - Minimum backup procedures such as retention period, periodic recovery tests, and offsite storage
    - Physical security of servers
    - For administrative data meet standards in UMD Policy VI-23.00(A)
  - Be audited by DIT security periodically to ensure compliance
- Changes Authorized in UMD Policies VI-23.00(A) and X-1.00(A)
  - “Policy on Data Management Structure and Procedures”
  - “Acceptable Use Policy – Security Standards”

Additional Possible Future Measures

- Consolidation of servers to AVW and/or CHR (Databridge Sites)
  - Provides increased:

    - physical security
    - more reliable power
    - better energy efficiency

- **Mandatory Advanced cyber training for local IT staff**
    - Likely a mix of online and in person training
    - May require payment for classes by local units
- **Mandatory use of DIT supported laptop/desktop backup service**
    - Cost are $100/employee/year

UMD VPN is a split tunnel, which means if you are working from your personal device and using the VPN, the VPN will only channel UMD business through the UMD VPN.

Richardson asked how much pushback is expected. Hollingsworth noted that, for example to Intune, life got easier as we got over the huddle of installation. There will inevitably be more work and questions on the front end.

Hollingsworth added that there will be a sense of loss of control on this. He hopes to communicate that this is just for the state funded university device, to calibrate to all the cyber risks there are. If we don't act, we will be acted upon.

Roy asks about the timeline and Hollingsworth said that they are just scoping the project now. DIT will do a risk informed analysis and then prioritize groups and sequence accordingly.

Approval of 01/08/24 minutes

Klauda moved to approve the minutes from the 01/08/2024 meeting. Roy moved the minutes for approval and Richardson seconded the motion. Voting members approved the minutes unanimously.

Vendor Contract Renewal Increase - Axel Persaud

Persaud briefly updated the IT Council by sharing that many of the vendor contracts that are up for renewal have proposed significant (up to 50%) increases in their renewals.

In some cases we are trying to reduce license counts and we are engaging with procurement on how we can push back.

We are also looking at temporary renewals, and we may present these issues as Agenda items for the IT Councils' strategic advice and discussion.

It is not just UMD, the BIG10 Alliance is also experiencing this. University budgets give Merit and COLA increases which do not go towards supporting increases in vendor contracts. Longer term contracts are the goal.

Appel noted that Educause should present a paper on this subject. There is a lack of awareness regarding what causes tuition increases. This is a major hidden cost when you compare costs today to what the technology was 25 years ago.

Klauda thanked the Council for their work and adjourned the meeting at 2:00pm.