FACULTY SENATE
SENATE ASSEMBLY
UNIVERSITY OF MICHIGAN

2022-2023 Information Technology Committee (ITC) Final Report

To: SACUA

From: Heather O'Malley, Chair, Information Technology Committee

Subject: Report on Activities of the ITC for 2023-2024

Advisory to: Ravi Pendse, VP for Information Technology and Chief Information Officer

Members: Heather O'Malley (Chair), Yasser Aboelkassem, Magda Ivanova, Yun Jiang, Zhixin Liu, Amir Mortazawi, Maura Seale, Sonia Tiquia-Arashiro, Varun Agrawal, Vivek Kumar Jaiswal.

SACUA Liaison (part year): Michael Atzmon

Meeting Dates:

- 5 full committee meetings: November 04, 2022; December 16, 2022; February 09, 2023; March 04, 2023; April 13, 2023.

Committee Charge

1. Continue to consider issues of Diversity, Equity, and Inclusion (DEI) in terms of service, delivery, and technical assistance and provide best practices for IT resources and their effective use for new project development among diverse populations on campus.

2. Identify financial, real, and perceived disconnects, deficiencies, and inequities in the populations on U-M campuses that are least served and need additional IT support to support faculty in-person and online instructional needs.

3. Consider best practices for faculty voting via online platforms (e.g., during Zoom meetings) to encourage expanded participation while still preserving secrecy and security of the vote.

4. Review whether the university's implementation of "Crowdstrike Falcon" raises any privacy concerns.

Summary:

The committee discussed a variety of topics related to this year's charge, with a particular focus on item #4, concerns regarding implementation of the Crowdstrike Falcon security platform, its capabilities, and faculty concerns around its use on campus.

We had one invited guest: Sol Bermann (Executive Director of Information Assurance and Chief Information Security Officer and Clinical Assistant Professor of Information, School of Information), to assist with technical and implementation questions regarding the capabilities of Crowdstrike Falcon.

Miscellany:

- The ITC received information from VP Pendse regarding major efforts and successes leading into this year, including WiFi updates, the Research Computing Package, cloud-based telephone function for central/Ann Arbor campus locations, and the Core Network Upgrade project.
- Several ITC members were able to bring up items of individual need (e.g. security for sensors used in a classroom context) and have these addressed with VP Pendse.

Primary Discussion Areas:

Cloud-based computing:

- Trends toward cloud storage and whether this presents a security concern
- Since cloud storage is replacing some local storage options, is a separate backup location then needed?
- Files uploaded to cloud (esp. Dropbox) that are deleted may then compromise local copies and lead to unintentional loss of files and data.
    - Dropbox may offer version control as a type of backup
- Options are needed for projects that require very large amounts of data storage
- VP Pendse detailed options (Dropbox team accounts, individual consultations for large storage needs) for storage beyond the new Google Drive limit of 250GB.

Crowdstrike Falcon:

- A committee member began the discussion with an account of having Crowdstrike installed on their computer by IT staff without being informed of its capabilities or that it could not then be uninstalled.
- Specific concerns regarding the capabilities of this platform: kernel-based, registry access, remote access, etc.
    - How often does UM software work at the kernel level?
- The committee discussed at length concerns regarding security of confidential documents that may be on faculty computers, including examples such as student records or confidential research documents.
- VP Pendse provided multiple examples of security breaches that have been successfully prevented or limited due to Crowdstrike capabilities.
- The committee expressed an interest in hearing from experts with differing perspectives on platforms such as Crowdstrike:
    - UM experts (VP Pendse assisted in suggesting UM's Sol Bermann, who attended the February meeting).
    - External experts from other institutions, or national organizations focused on cybersecurity and related issues.
- Not all units across the three campuses deploy Crowdstrike.
    - Which units use this platform? (See below section for more information.)

    - How many faculty computers is it installed on? How many staff computers or shared computing stations?
    - Have any units moved away from Crowdstrike, and if so, to what?
    - How much deployment of Crowdstrike (percent of computers, percent of coverage, etc) is needed for it to be effective? Are there specific network locations where this is more essential?
- The University cannot require students to have Crowdstrike installed. Why is this different for faculty?
- A "backstage" demo of Crowdstrike capabilities was offered but (as of May 2023) had not been scheduled. (It may occur in the summer, schedules permitting.)
- Some peer institutions are having similar discussions including discussions of a parallel platform (CORTEX) which is raising questions regarding faculty privacy, so this discussion extends beyond UM.
- The main AAUP website has a statement available (AAUP Academic Freedom and Electronic Communications) which is useful although slightly dated (posted in 2014).

Notes from invited guest Sol Bermann regarding Crowdstrike:

- Both VP Pendse and Sol Bermann have individually worked on projects related to IT privacy. Sol teaches a class on privacy and surveillance. ITS has been developing a dashboard on student, faculty, and staff privacy (ViziBLUE) and are interested in creating a UM privacy think tank.
- CrowdStrike is deployed on all three campuses and on Michigan Medicine. Some units (e.g. Ross, Engineering) run their own subtenant. UM is one of the largest deployments of Crowdstrike with the tool on nearly 100,000 devices. The UM license does not include personal computers. The license covers UM supplied computers and servers.
- CrowdStrike works by flagging suspicious activity and blocking it. If the suspicious activity is determined to be legitimate, ITS will release the blocked code or software. By isolating the suspicious activity, Crowdstrike prevents the spread of malware and other threat incidents.
- CrowdStrike is just one tool used in a layered process of IT security at UM.
- CrowdStrike does have the capability to see and delete files and to install programs. However, like other programs (including Gmail and Slack), IT staff would require a request from appropriate authorities to do an investigation, i.e. procedures through the general counsel's office where such a process would also be documented.

General security questions and concerns:

- Should the University be able to monitor or access items such as email or files?
- Most IT vendors do have access to data (Google, Microsoft, etc), and it is the strict policies of those vendors and of UM that prevent access to faculty data.
    - Is there sufficient trust in these policies for faculty to feel secure in their privacy?
    - Example: when past-President Schlissel's emails were made available online, which is at odds with a strict privacy policy. This also eroded faculty trust.
    - Patriot Act and other subpoenas can lead to release of data

    - Positive example: UM Library's opt-in policy for storing library checkout records
- UM does contribute to community outreach: VP Pendse's office has an initiative of a boot camp to help local schools prevent data breaches
- Costs for cybersecurity insurance are significant (and increasing) and UM is investigating options.

Zoom meetings, open discussion, and voting:

- Implementation of SimplyVoting and also UM voting site (vote.umich.edu) have resolved issues with voting following remote/hybrid meetings
- Potential invited guest for the future: Bob Jones to discuss accessibility in meetings, both in general as well as for large Zoom meetings (such as full Faculty Senate meetings).

IT Equity across Campuses:

- VP Pendse's office does not have jurisdiction over the Dearborn or Flint campuses. Are there actions the ITC or SACUA could take to promote and ensure IT equity and access on all three campuses?
- This should involve discussions to avoid duplications of existing software or structures (this also applies to the 19 Ann Arbor units).
- ITC members are encouraged to contribute to President Ono's visioning process leading us toward 2034.
- The focus group report from 2021-2022 submitted by past Chair Rachel Vacek contains a great deal of relevant information that is worthy of ITC follow-up.

Suggestions for 2023-2024 from VP Pendse:

- IT Visioning for 2034 is an opportunity for faculty input on IT issues.
- A new version of UM's enterprise resource planning (ERP), e.g. Peoplesoft, that includes payroll, student transcripts and more. This is a very large project for IT and UM's current system is highly customized from the vendor version and will require much testing for a good transition. There may also be opportunities for increased collaboration with UM-Dearborn and UM-Flint on this project.
- IT support for research computing, including generative AI.

Recommendations:

1. To improve equity across all three campuses, the current system where the campuses are functionally independent may need revisioning. As of this report, the Ann Arbor campus lacks authority to cause change when needed or optimal for the other campuses. A more collaborative approval or decision-making structure may be beneficial. This would allow the Flint and Dearborn campuses to benefit from the extensive resources, such as licensing agreements, present on the Ann Arbor campus.
2. Crowdstrike Falcon implementation has had demonstrated successes in protecting the University from cyber-attacks; however, there remain concerns among faculty regarding the

capabilities of this platform and how it may affect them. VP Pendse and ITS have made significant efforts to increase transparency and therefore promote trust regarding this platform. Providing information openly to faculty who use UM-owned/managed computers about the use of Crowdstrike Falcon and offering opportunities to ask questions may be beneficial. It may also be beneficial to provide a mechanism by which faculty with sensitive information or strong objections can have access to alternative computing resources without compromising UM cybersecurity.

3. Pursuant to point 2, UM SPGs related to IT policy should include specific mention of the use of any form of monitoring platform or software that can perform such functions and if these programs are installed on computers designated for individual use, the processes by which data could be accessed, and the consequences of malfeasance, if these documents do not already contain these details.