FACULTY SENATE
SENATE ASSEMBLY
UNIVERSITY OF MICHIGAN

Ruthven Building
1109 Geddes Avenue, Suite 1120
University of Michigan, Ann Arbor, MI 48109-1340

Information Technology Committee (ITC) Minutes

Meeting Date: February 9, 2-3 pm (regular meeting)
Circulated: 03/03/2023
Approved: 03/09/2023

Present: Heather O'Malley (Chair), Ravi Pendse (VP for Information Technology and Chief Information Officer), Vashni Santee (Executive Assistant to VP Pendse), Yasser Aboelkassem, Vivek Kumar, Yun Jiang, Magda Ivanova, Zhixin Liu, Ann Marshall (FSO, Secretary), Amir Mortazawi, Maura Seale, Sonia Maraya Tiquia-Arashiro

Invited guest: Sol Bermann, Executive Director of Information Assurance and Chief Information Security Officer and Clinical Assistant Professor of Information, School of Information

1. Meeting called to order at 2:05 and minutes from December meeting were approved.

2. Links about CrowdStrike Falcon provided by Sol Bermann are appended to the minutes.

3. The meeting was a Q & A format with Sol Bermann as invited guest to provide insights on CrowdStrike Falcon. Issues discussed include:

- Both VP Pendse and Sol Bermann have 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.
- There was a discussion about how Crowdstrike is useful in preventing and/or solving threat incidents in a campus environment.
- 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.
- IT has partnered with faculty in Engineering who are working on research about internet equity and access.

4. Next meeting is Thursday, March 9th, at 2 pm

U-M Links (Public) Provided by Sol Bermann in Advance of the Meeting:

- Enhanced Endpoint Protection for U-M Computers - High level overview of why we use advanced endpoint protection, and some of the safeguards around its use
- Endpoint Protection: Data Collection, Sensitive Data, and Privacy - Deeper dive into what data Crowdstrike Monitors and Records, and does not monitor and record, and a reiteration of the access and privacy safeguards
- CrowdStrike Falcon FAQ - FAQ version that reiterates some of the above docs and takes a deeper dive into other questions
- CrowdStrike Falcon for Units - Describes unit use of Crowdstrike (if they run their a sub-tenant)
- Crowdstrike IT Symposium 2020 Poster
- ITS Information Assurance IT Security Community Newsletter Article on Crowdstrike Deployment (Winter 2021)
- Mich Med Crowdstrike Deployment Announcement (Oct. 2021)

- ITS Information Assurance IT Security Community Newsletter Article on Crowdstrike Deployment (Summer 2022)

Respectfully submitted,

Ann Marshall (FSO, Secretary)