APPROVED ANNUAL REPORT
Computing and Information Technology Committee (CIT)
AY 2020-2021 and AY 2021-2022
Professor Deirdre Mulligan, Chair

In fulfilling its charge as established in the Bylaws of the Berkeley Division of the Academic Senate, the Committee on Computing and Information Technology (CIT) carried out the following activities. The chair of CIT during both AY 2020-2021 and AY 2021-2022 was Professor Deirdre Mulligan.

Chair's summary: The two years covered by this report represented a historical increase in the importance of computing and information technology due to the emergence and ongoing presence of the pandemic. The movement of classes and other campus business activities almost exclusively online at the beginning of this period and the high-stress reintegration of students, faculty, and staff at the end of this period (bringing more WiFi-connected devices back than had ever been seen on campus before) exposed a variety of weaknesses in our infrastructure and growing needs moving forward.

CIT had several briefings from CTO Jenn Stringer and her staff on the state of IT—including WiFi, contracted services (Box, Google, etc.), shared infrastructures (such as the Accellion File Transfer application at issue in the Accellion breach). These prompted conversations around challenges including: housing growing IT infrastructure on campus, deferred maintenance and updating, and potential synergies or opportunities for collaborations with the labs.

During the periods in question, the CIT committee worked to stay abreast of issues as they arose and further established three subcommittees to focus on a range of short- and longer-term priorities. Two major issues that arose were (1) The Accellion breach and (2) major issues with the newly installed WiFi infrastructure. A summary of committee activities is given below. The outcomes from the three subcommittees are given afterwards.

I. ADVISORY ACTIVITIES

A. Accellion Breach

CIT was briefed on the Accellion breach and was in regular contact with the CISO, Allison Henry, and CPO, Scott Seaborn, to provide advice and support for their activities to address risks to the campus community. Based on those briefings and input from campus stakeholders and experts CIT invited in to provide briefings, CIT advised the faculty senate about measures necessary to address current and future risks to the campus community.

On May 5, 2021 CIT sent a memo to DIVCO expressing concerns about: University of California, Office of the President's (UCOP's) handling of notifications surrounding the Accellion security incident, and concerns about adherence to systemwide policies that will likely make the impact of this breach catastrophic for some portion of the Berkeley community. In particular CIT raised concerns with UCOP's compliance with system-wide standards for handling and monitoring PL4 data.

We observed that UCOP's notices to the campus community did not adequately notify individuals about the sensitive data affected by the breach which posed potential safety as well as privacy risks to community members and their families. We also observed that UCOP's communication with campus lacked the details necessary for campus to assess the impact on UCB security posture and adopt appropriate mitigation strategies.

After receiving a response from the UCB Incident Response team, with whom the Committee has a strong relationship, CIT sent a follow-up letter on June 23, 2021, emphasizing that our concerns were about UCOP's response to the breach, not the UCB campus's response, and requesting that DIVCO or UCOP provide additional information about whether and how our other concerns were being addressed. No response was received.

B. WiFi network recharge

During AY 2021-2022, the WiFi network received a much-needed, campus-wide recharge. The recharge was not without issues, however. Over a series of meetings, the CFO provided historical information on the campus network recharge model and the Wi-Fi network. The significant WiFi disruptions in Fall of 2021 underscored the need for greater attention to IT as a common and necessary good and the need to establish stable and equitable financing models to sustain the level of service appropriate to support UCB caliber research and teaching. We discussed the need for increased communication with campus stakeholders and the need to gather data about ongoing experiences once the Arbua update was complete.

This led, in part to the creation of the:

- Wi-Fi Fall issues webpage. This is a detailed account and FAQ on the issues the campus has experienced.
- Network User Improvements Program webpage. This describes the IT Top Priority program to improve the overall experience of network users on campus. The goal of this project is to offer a broader and clearer range of connectivity options and to modernize and improve the capacity of various network services where necessary.

C. Additional activities

In addition to the two principle issues mentioned above, CIT also reviewed, discussed, and provided input on:

- New IS-12 policy. CIT invited Allison Henry, Chief Information Security Office, and Professor Anthony Joseph, the campus Cyber-risk Responsible Executive, to discuss IS-12 and it's interaction to IS-3. CIT provided comments to BDAS on Feb. 1, 2021 reflecting the Committee's recommendations to the Information Security Office and the resulting changes.
- Minimum Security Standards for Networked Devices (MSSND). The committee reviewed the updated draft, concerns raised by faculty and staff across campus, and discussed the revision with CISO Henry. CIT found that the revised draft addressed substantive concerns and had no further comments.
- Java log 4j Vulnerability: after a briefing from CISO Allison Henry in which the risks posed by the vulnerability, the difficulties of communicating due to impending curtailment, and the need for patching across multiple systems were discussed, CIT advised sending a Cal message as well as messages to technical leads on campus.
- UC Presidential Working Group on AI: CIT invited Brandy Nonnecke to brief the committee on the activities of the UC Presidential Working Group on AI. She described the strategic goals of this working group as well as its methods, including literature review, survey of campus CIOs and CTOs, and interviews. She also discussed the structure and workings of the Group and its Subcommittees on health, human resources, policing and student experience. The final report is given here: UC AI Working Group Final Report. Given potential synergies, CIT recommends that the findings and recommendations of the Subcommittee on Fostering integration of accessibility, privacy, security, and equity analysis into IT procurement and development (described below) be shared with campus staff responsible for implementing the UC Responsible AI principles.

II. CIT SUBCOMMITTEES ON FUTURE CONCERNS

A. End of Free: What is the impact?

CTO Jenn Stringer alerted us to the pending end of "free" services as software companies and service providers, such as Box, Google, and Microsoft, move to a subscriptions-based model. The impact of reducing, removing, or eliminating unlimited services and free "cloud credits" pose a range of concerns for the University. Some of the terms are being dramatically shifted, creating a source of instability in IT planning. Service providers are attempting to force universities into a higher tier of service. Limits on or the disappearance of free cloud credits pose challenges for teaching and research practices that have become dependent on them. After a detailed presentation on this issue from Luis O. Hernández Director of Productivity and Collaboration Services, the CIT decided to form a subcommittee to explore the issue and provide guidance to the Faculty Senate.

The End of Free subcommittee, John Kubiatowicz and Matt Welch, with support from campus subject matter expert Luis Hernandez, gathered information and generated recommendations for the CIT consideration. The subcommittee noted that campus should gain a clearer understanding of unlimited resource usage. The experience with BOX revealed the difficulty of understanding campus usage of free services and the difficulty this gap creates when a vendor shifts fee structures. The subcommittee believes campus should gather information proactively and believes this issue are increasing in magnitude and urgency.

The Subcommittee suggested that, while there were a number of on-campus groups working toward solutions of individual issues (notably the Productivity and Collaboration Tools Committee as well as the CTOs office), they suggested that there might be a role for CIT to weigh in on policy questions, and to recommend data and information to support campus decision making. Key policy issues identified include:

- Figuring out minimum University or Department-level storage or compute credits? And considering who would pay?
- Policies to ensure sufficient duplication of service to avoid disruptions
- Policies and practices that enable proactive data collection about usage and needs to be well situated to respond to understand the implications of and respond to vendors shifts in pricing and services

B. Fostering integration of accessibility, privacy, security, and equity analysis into IT procurement and development

This second subcommittee was established in response to issues about privacy, security, accessibility and academic freedom arising during the move to remote teaching and the increased reliance on private platforms to support learning. The move online emphasized the connection between campus obligations and commitments to accessibility, privacy, security, and academic freedom and the technology we procure to support the teaching and learning environment. The committee produced a fairly substantial set of recommendations of ways in which some entity (perhaps CIT) could assist in improving the overall state of the Berkeley infrastructure.

This subcommittee consisted of Kimiko Ryokai and Jeremy Nicolai, with support from campus subject matter experts Scott Seaborn, Campus Privacy Officer, Charron Andrus, Associate CISO, Ella Callow, ADA/Section 504 Compliance Officer, and Erfan Mojaddam, Director of DevOps and Learning Spaces, explored whether CIT might play a role in ensuring the University's values fully inform technology brought into the teaching and research environments. In particular, the Subcommittee considered whether campus would benefit from a review mechanism related to academic freedom in the procurement process. They also considered whether CIT might play a role in helping faculty understand the importance of the vetting done by UCB staff subject matter experts and the risks that can flow from the prevalence of bespoke technology solutions (e.g. BYOT, or "bring your own technology") brought by faculty into the classroom environment without sufficient review or evaluation through the normal procurement process.

The Subcommittee made three high level recommendations for work CIT could recommend to the Faculty Senate:

- Documentation (posted in location that's easily findable by instructors):
    - Publish information on the web that outlines the policies, processes and reasoning for compliance with each of the areas: accessibility, privacy, security, academic freedom
    - Provide a listing of good and bad technology options and vendors who are experienced with creating compliant sites and systems for UC Berkeley
- Provide faculty and others with pointers to relevant Experts on campus
    - Expert(s) should be designated/identified who can answer questions and provide guidance for each of the areas
    - Support contact information should be posted on the page
- Training on these issues for instructors through multiple avenues:
    - Orientation for new instructors
    - Trainings through departmental meetings
    - Self-paced training posted on newly created webpage and/or UC Learning Center (Learning Management System)

The Subcommittee also provided analysis of challenges and recommendations with respect to Accessibility, Privacy, and Security. More details are available upon request. In summary, the subcommittee noted the dangers of not adhering to campus policy is an unfortunate perpetuation of non-compliance: employees will continue to purchase and utilize technologies that are inaccessible, subject to privacy breaches and generally insecure. Specifically with respect to Privacy, it was noticed that there is a significant danger of failing to comply with relevant privacy laws, including the Family Educational Rights and Privacy Act (FERPA), the Information Practices Act (IPA), the General Data Protection Regulation (GDPR), the UC Policy on the Protection of Personally Identifiable Information (BFS-RMP-7); also a failure to provide adequate notice to students regarding how their data is used, obtaining consent before sharing personal data with third parties and to abide by UC Berkeley's prohibition on selling of student data

The subcommittee suggested that CIT could help overall Accessibility by encouraging employees to review and understand the basic requirements of the UC Information Technology Accessibility Policy and the Implementing Procedures as well as take advantage of campus resources, such as WebAccess clinics, early in the process of developing new infrastructure. The subcommittee also suggested that website administrators should be encouraged to migrate websites to OpenBerkeley if at all possible, as well as take the LMS SiteImprove series on designing and operating accessible websites. They also suggested that all websites should be audited regularly with SiteImprove, that keyboard navigability should be manually tested regularly, and all video content should require captioning.

With respect to Privacy, the subcommittee suggested that CIT could help overall through communication:

- The Privacy Office can provide a privacy vendor assessment checklist to the CIT which the CIT can distribute broadly to the faculty community.
- CIT can assist in communicating the need to consult with the Privacy Office when acquiring any software that will be used with student data.
- The CIT can host a Faculty Software Acquisition Guide/Portal (mirrored after Research IT's Research Data Portal) that can serve as a one stop shop for faculty looking to purchase software and which includes relevant requirements and recommendations for each subject area [Accessibility, Privacy, Academic Freedom, Security, Training and Support, etc.]

With respect to Security, the subcommittee suggested that CIT could help through communication and outreach, specifically:

- CIT can help with communicating the importance of understanding and adhering to the MSSEI and MSSND policies to ensure compliance with relevant laws, including HIPAA, FERPA, PCI-DSS, GLBA, NSMP-33, CMMC 2.0 for DoD funded research, 800-171, etc.
- CIT can assist with outreach and education on the bIT Software Website used to educate on available enterprise solutions
- CIT can encourage Supply Chain Management to make changes to the BearBuy form to support not only Security but also Privacy and Accessibility
- CIT can help socialize the importance of adherence as it relates to our ability to obtain affordable cybersecurity insurance

C. Accellion Breach: Moving forward

CIT established a subcommittee, Deirdre Mulligan, Paul Schwartz, Anthony Joseph supported by campus subject matter experts Allison Henry and Scott Seaborn, to consider additional issues surfaced during the Accellion breach, specifically concerns with the stewardship of UCUES (student survey) and campus survey data generally and UCB visibility into UCOP practices that affect UC individuals' data.

Issues discussed included how the UCUES survey was administered and how the data was stored. CIT in conversation with campus experts discovered that UCOP survey administrators did not segregate survey answers from participants, did not encrypt the participants identifying information, collected answers to broad questions in free text fields, and did not discard identifiers once they were no longer necessary. CIT discussed the risks to the UC mission posed by UC wide and campus administrative surveys not meeting standards expected of campus researchers. We learned that the campus privacy office was advising the UCB OPA on data segregation and minimization practices and that they had agreed to have the OPHS review their data collection practices even though their surveys are not technically human subjects research. We also learned that UCOP Privacy had made a similar recommendations to the UC wide student survey administrators. CIT understands that various offices conducting surveys, including IRAP, OPA and People and Culture, have agreed to run survey question/protocols by an IRB and the Privacy Office, and that the subsequent UCUES (University of California Undergraduate Experience Survey) survey questions were reviewed by the UC IRB. We understand that there are ongoing efforts at the UCOP level to ensure appropriate privacy and security standards are in place.

The Subcommittee recommends that CIT request DIVCO reinforce efforts to improve the privacy and security practices covering administrative survey data across the UC system.There are a number of student and employee surveys conducted each year and the exposure of sensitive survey data collected by the UC may not only put campus community members at risk but it may also reduce trust in the data collection and handling practices of UC researchers engaged in human subjects research. Campus stakeholders and the broader public are unlikely to distinguish between survey data collected for administrative and research purposes, so CIT supports efforts to provide consistent processes for ensuring the privacy and security of survey data collected by the UC.

The Subcommittee also reviewed the recommendations from the Orrick investigation of the Accellion breach. The recommendations were provided to UCOP in Spring 2022 and CIT is unaware of the extent to which they have been implemented. While the Subcommittee found many of the recommendations appropriate, members emphasized the need for UCOP to ensure local staff have the information necessary to identify local risks and mitigations and raised concerns about centralization that could further reduce access to information. This was a key issue in the Accellion breach, as identified in the CIT letter to DIVCO of May 5, 2021. The Subcommittee recommends that CIT follow the adoption of the recommendations and seek additional information responsive to issues raised in our May and June letters.