



UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING AND COMMUNICATIONS

December 13, 2024

Meeting Minutes

I. Chair's Welcome, Agenda Review, Approval of Minutes

Action taken: Meeting minutes from October 4, 2024, were approved.

II. Consultation with UCOP Administrators

1. Information Technology Services

As requested, Cyber-Risk Program Manager (and Interim CISO) Monte Ratzlaff provided data on the causes of cybersecurity incidents at UC. UCACC was able to see a graph that categorized 78 incidents from 2024 by type (e.g., ransomware, human error, phishing, stolen or lost information, etc.). A few incidents may have been counted in more than one category. The graph can be compared to previous years to show change over time; for example, the number of reported ransomware incidents in 2024 was higher than in 2023. UCACC members thought that a report showing the impact on operation or cost from breaches in the various categories would be useful. The total number of attacks per year is in the millions, with even more alerts that are just "noise." Members suggested that understanding the attack vectors could be useful in allocating resources. Ratzlaff will share more about the incident escalation protocol and how an incident makes it onto the chart. Generally, these include breaches that included sensitive data, required coverage, impacted more than 10 individuals, would invoke litigation or investigation, involved known criminal activity or a nation-state, or required ransom payment.

It was a security breach in 2014 that kicked off the current focus on cybersecurity. The cost was well into multi-million dollars, including litigation and subsequent controls. Committee members expressed concern about ransomware and the bigger impact on research data, specifically. Protecting important research data involves resources, including backup strategies. "Training" is often invoked, but training fatigue is growing. Related to the UC Cybersecurity training, members asked whether the videos could be more specific for the university context. Better communication could also help to raise awareness and get buy-in for the needed protections. Faculty should clearly understand that the training and security requirements protect them and their work. Narratives of actual situations might help to make it more real and personal and would help both students and faculty understand that cybersecurity is in their best interest, and not just in the interest of the university. Ratzlaff noted that is replacing the current training in the next year or two and anticipates moving away from compliance-based to just-in-time or error-based efforts that are user-specific rather than legalistic. UC Berkeley is piloting faculty-centric approach for mandatory training. To get students onboard, it might be worthwhile to explain how easy it can be to protect your data and identity. Many tools, like bio-IDs or passkeys, can be easily integrated into existing technologies.

Committee members discussed metrics for cybersecurity efforts, including training. There is still interest in more metrics of the efficacy of EDR, training videos and other mandated controls. It is understood that with rise of LLMs and AI tools, phishing will become even more sophisticated and harder to detect.

Members discussed differences in communication and responses to President Drake's February cybersecurity letter. In most cases, faculty have not heard of the plans or the mandate from UCOP. Local Senate discussions with CISOs and CIOs should be taking place, and information disseminated, as much as possible.

Action: Committee members will review the revised draft EDR and MFA standards to discuss at the next meeting.

2. IT Strategic Sourcing

Roshni Pratap, Director of IT Strategic Sourcing, joined the meeting via Zoom to provide updates on UC's agreements with OpenAI and Adobe.

OpenAI – UC has systemwide licenses for ChatGPT Enterprise and ChatGPT EDU. UC agreements have strict controls on data, including use and retention, and prohibit offshoring of data. OpenAI has informed UC that it is currently unable to fully meet the US data residency requirement and has requested a revision to allow broad discretion to offshore data to jurisdictions not subject to sanctions. This applies to both ChatGPT Enterprise and ChatGPT EDU. OpenAI has indicated that it is working on adding US residency, but no confirmed timelines.

OpenAI has proposed revisions to its agreement that would permit the company to process or access UC data, including regulated data such as PHI and educational records, in unknown jurisdictions at their discretion. This is in direct conflict with UC policies prohibiting the offshoring of sensitive data. Given the significant risks, CISOs, CIOs, or chancellors must be consulted prior to any further engagement with OpenAI. IT campus leaders – CIOs, CTOs, CISOs – are aware of the issue. UC locations do have other options for AI licenses, such as MS Copilot, Google's Gemini, and Vertex Enterprise which are compliant with UC's policies.

Director Pratap suggested that a statement from the Academic Senate about the lack of data controls would be useful in UC's dealings with OpenAI.

Adobe – Since 2013, UC has maintained a systemwide contract with Adobe for Acrobat and Creative Cloud. The agreement was demand-based, with pricing disparities between site license and named user type license. Only a few campuses (UCB, UCLA, UCSC) currently have Adobe site licenses that extends access to their students.

UC recently negotiated a new agreement with Adobe based on a UC-wide site license model, with a single payment based on a consolidated pool of licenses. The new model significantly reduces the unit cost across all licenses, keeps total systemwide costs stable, and expands the number of student licenses with an addition 100,000 available. However, the UC system lacks a means to fund and manage student licenses for Adobe products without resources to support receiving requests and provisioning student licenses. For the initial year ending in June 2025, Central IT has absorbed the cost of student licenses. Volunteers are sought to help develop an equitable and affordable solution for providing student access to Adobe products.

In discussion, committee members mentioned the responsibility of faculty to provide tools to students that they think students should use. Assigning specific software tools sends a message and faculty should be thoughtful about what they select. For example, NotebookLM is a new Google product that is widely available and bills itself as a “research assistant,” but may not be appropriate for student use.

If use of OpenAI products are no longer recommended – by either faculty members or UC policy – that needs to be communicated clearly and quickly.

III. Reports from other committees

- UC AI Council update

UCSF Duygu Tosun-Turgut is the Senate representative on the UC AI Council. She noted that the Council discussed OpenAI and potential AI legislation in California regarding the safe and effective use of AI. Members asked whether there would be a call to UC faculty for input.

The AI Council’s Workgroup on Risk Assessment has continued to work on the AI risk assessment guide for AI procurement and is now developing case studies. Ultimately, assessment will be conducted locally, although following systemwide standards.

- Faculty AI Workgroup update (Lisa Yeo & Igor Mezic)

The Academic Senate has convened a systemwide Faculty AI workgroup to focus on topics that are within faculty purview. The 13-member group includes representatives from systemwide committees (including UCACC) and almost all of the campuses. One of the first actions will be a survey conducted in conjunction with the administration to collect information on faculty AI uses and attitudes. (Students are already surveyed on AI via the bi-annual UCUES survey.) The faculty will divide into subgroups covering instruction, research, admissions, and data stewardship

IV. Senate Leadership Updates

Academic Council Chair Steven Cheung joined the meeting to provide updates on the current issues facing the Academic Senate.

- *Board of Regents November Meeting*

- At the November Regents’ meeting, the board approved a budget of over \$55 billion that includes a 9.9 percent increase in tuition for out of-state students, \$1.4 billion for seismic projects and deferred maintenance, and a 3.7% range adjustment increase to scale salaries. UC’s investments continue to do well, and the time to get to full funding of UCRP (retirement program) has been shortened to an estimated 17 years now. Health care premiums continue to increase.
- UC Regent John Perez will be replaced by Los Angeles sports media executive Bob Myers.
- Former Executive Vice President for UC Health gave a presentation describing UC’s success in handling the Covid pandemic.

- The union representing UC graduate students agreed to a contract extension through January 2026 (rather than May 2025).
- The UC MOP mortgage loan assistance program will receive an infusion of \$100 million in January 2025, with distribution to campuses based on need.
- At yesterday’s meeting of the Assembly of the Academic Senate, UCEP’s updated UC Education Quality statement was approved. Assembly members considered a new admission requirement to augment the current A-G. There was lively discussion and a vote was postponed to April.

- Executive searches are underway for UC President, UC Education Abroad Program Director, UCSB Chancellor and UC Riverside Chancellor.
- *Workgroups*
 - o The APC Workgroup on Systemwide Academic Calendar has met three times and is finalizing an input form to gather information on how constituents feel about some of the potential aspects of a semester calendar. The results of the initial survey will be used as preliminary feedback to inform discussions of various models. UCI Professor Don Seneor, the former chair of UCPB, will be the Senate's representative on the cost assessment sub-group. A systemwide review of the workgroup's recommendations is expected in late spring.
 - o The workgroup to review APMs 015 and 016 was convened to fulfill a statutory requirement of the CA Budget Act that required review of policies around administrative responses pertaining to free expression and community safety. The workgroup has so far found that APM 015 is sufficient and is not proposing any changes. It will likely recommend the development of guidelines like those for SVSH (sexual violence and sexual harassment), to address freedom of academic expression and related questions.
 - o The APC Workgroup on Doctoral Education, which was convened last year, is wrapping up its work. Co-chairs Susannah Scott (previous UCSB Academic Senate Chair) and Gillian Hayes, Vice Provost for Graduate Education and Dean of the Graduate Division at UC Irvine reviewed the group's report and recommendations at the October Academic Council meeting and will collect feedback from systemwide committees and others before the report is finalized.
- UC HR is conducting a total remuneration and benefits review that will be complemented by a separation study. There will be Senate representation on the workgroups that will help guide the process and ensure that it is consistent with past reviews.

V. Campus Issues and Committee Discussion

UCACC members discuss the relevant academic computing and communication topics from their divisional committees and campuses. Note that UCACC maintains a [shared chart](#) for information and comparison of campus IT governance structures.

UC Berkeley is continuing to implement the requirements of President Drake's cybersecurity mandate. The latest proposal has been to revamp campus-wide networking to enable endpoint-knowledgeable subnetting, which will help with restricting content. The campus is developing requirements that will include how privacy protection. Only UC-managed hardware has been included so far. Issues around data storage continue, including a pilot to use the NASA Ames site. Berkeley has a new mechanism for proposing infrastructure changes that goes through IT committees and then the Senate IT committee. One proposal is to use an AI tool from a Berkeley startup for some staff hiring. Proponents say it will be less biased.

UC Santa Cruz is trying to implement the new security mandate, but the timeline is getting challenging. Santa Cruz is facing budget issues and is mindful of equity in IT budget and staffing. The faculty need guidance, but apparently the delay in communication is out of caution – so that the administration release anything that will later need to be retracted. The faculty Committee on IT, in conjunction with the CISO, has worked on a FAQ. (A draft can be shared with the committee.)

UC Santa Barbara committee discussions have covered: cybersecurity, research data security, data management, and AI use and misuse. Faculty are concerned about mandates for software on private devices. There was some thought of creating a cybersecurity committee separate from CIT.

UC San Diego discussions have focused on artificial intelligence. There have been multiple reports, recommendations, a policy, etc. A “secure connect” initiative responds to President Drake’s cybersecurity letter with efforts such as EDR, network access rules, more frequent timeouts, and cybersecurity training. There might be more aggressive actions - like restricting access if you haven’t done training – in the future. The student information system (new course proposals, financial aid, student records) is being overhauled, with some trepidation.

UCLA faculty have lost some of their Google storage space. Exceptions are available, but there is little communication from IT to rest of campus. UCLA has achieved greater than 80% cybersecurity compliance, although many faculty are stridently opposed to EDR software. Conversations around compliance with the President Drake mandate are ongoing and include exception processes. AI issues are ongoing, with the campus offering Co-pilot, Gemini, and OpenAI. Regarding the new Accessibility Policy, it is likely that faculty will reduce course content.

UC Riverside has undergone an IT governance revamp, with an IT Strategy Council at the top. Many are excited about AI possibilities, and the campus has licensed Gemini, Notebook, Model Garden (vertex AI with an assortment of AI language models). IT is trying to get “software distributed access” (SDA) to networks which allows customization and granularity. Ready in 2027! The CIO and CISO don’t appear to have any kind of marketing strategy in place for cybersecurity updates, but a communication plan is coming soon.

UC Merced’s cybersecurity marketing strategy is dubbed “ProtectUs.” The campus has discontinued its own wifi and will use only Eduroam. The SSO (single sign-on) process will take action if a user is not in compliance. The first step is to inform, and then it will redirect in subsequent attempts. The Senate IT committee, FACIT (faculty advisory CIT) has a gap in that there is no representative for research computing. Research data protection and infrastructure is becoming a bigger issue, with federal rules coming soon.

UC Irvine has no stand-alone CIT, only CORCL (Committee on Research, Computing, and Libraries), and although none of the members are really engaged with IT, the committee has frequent interactions with and presentations from IT administrators on issues such as email and endpoint protection. The UCI cybersecurity response is a work in progress. For generative AI purposes, UC Irvine has ZotGPT, which is supposed to be campus-specific. A recent issue was the engagement of Deloitte to assess IT and make strategy, and whether this was the best use of resources.

UC Davis: The faculty committee is trying access the campus Information Security Management Program but have been told by the CISO that the document is confidential. This has set up a situation where faculty need to be educated about cybersecurity responsibilities but cannot find out what they are. UC Davis is doing well on training compliance; the biggest barrier is student employees, who are more transient. The campus is looking to implement physical tags on every device for compliance with EDR standards. Other topics of discussion are academic integrity related to AI, research attestations and NIST 800 171 – the protection of Controlled Unclassified Information (CUI). Anecdotally, the

Oracle transition that began at the beginning of the year has resulted in accounting errors, inaccurate account balances, and inability to access accounts.

The graduate student representative noted that access to the Office365 app was lost.

The undergraduate student representative said that loss of storage space was a big issue. She also noted that UCLA's large Ethnomusicology program has run out of physical space and so is now turning to digital out of necessity.

VI. Wrap up and Next Steps

- Obtain more details about reporting breaches and how an event rises to the level of inclusion in the pie chart displayed in the meeting.
- Follow up with IT Procurement about issuing a statement from the Academic Senate regarding OpenAI and data security.
- Obtain draft FAQ from UCSC on cybersecurity plan activities.
- Committee members review revised draft EDR and MFA standards to discuss at the next meeting.

Meeting adjourned: 3:00

Meeting minutes drafted by: Joanne Miller, UCACC Committee Analyst

[Attest: Jenson Wong, UCACC Chair]

Meeting participants:

Jenson Wong (Chair, UCSF), George Porter (Vice Chair, UCSD, via Zoom), John Kubiawicz (Berkeley, via Zoom), Jeremy Mason (Davis), Paul Gershon (Irvine, via Zoom), Irene Chen (UCLA, via Zoom), Lisa Yeo (Merced), Ilya Brookwell (Riverside), Barry Grant (San Diego), Duygu Tosun-Turgut (San Francisco, via Zoom), Igor Mezic (Santa Barbara, via Zoom), Jerome Fiechter (Santa Cruz, via Zoom), Katia Hatem (Graduate student, UCR), Aatmi Mehta (Undergraduate student, UCLA), Steven Cheung (Academic Council Chair), Kathrin Plath (Ex-Officio, UCOLASC Vice Chair, via Zoom), Monte Ratzlaff (Cyber-Risk Program Manager/Interim CISO, via Zoom), Roshni Pratap (Director of IT Strategic Sourcing, via Zoom), Joanne Miller (Committee Analyst)