Cyber Security at UC San Francisco:

In June 2015, the UCLA Medical Center suffered a cyber-attack in which hackers stole up to 4.5M personal records, which included financial information of patients from the Medical Center. In fact, these intruders entered UCLA's network outside of the medical center, and appeared to be hunting for intellectual property but were able to make their way to the Medical Center. As is often the case, the valuable data were not medical in nature, but rather financial identifiers, which can be readily sold on a cyber-black market. Apparently some patients have experienced identity theft, perhaps related to this breach.

"I am concerned about the possibility in the future of excessive oversight by the UC administration and efforts to monitor faculty productivity without the knowledge of faculty members. My concerns are about the loss of privacy to UC Faculty and being monitored in terms of how time is spent. I definitely also highly concerned about external intruders, at a global level, and our vulnerability as a society (not just UCSF) to cyber terrorism."

This breach shares features in common with many cyberattacks, including a recent breach of campus financial records at UC Berkeley. Often an intruder gains access by a direct attack on a server, or via phishing mail opened by someone on the campus network. The opened phishing document leads to download of malware that establishes a beachhead on a local server, which then can launch a high volume of attacks on other servers within the network. Intruders can meander through the system attempting to gain access to new servers and their data. Ransom attacks feature a specific type of malware that encrypts data, enabling the intruder to demand payment in order for the data to be decrypted. Ransom attacks have been waged against individual computers at UC campuses. Within a network, like in a kitchen, one person with poor computer 'hygiene' behavior, can compromise a multitude of other users.

The UCLA and UCB break-ins served as a wake-up call to the University of California, as shortly thereafter UC President Janet Napolitano has formed an external cyber security group, and hired the cyber security firm Fidelis on a temporary basis (FireEye) to monitor external cyber threats across the UC system. This system includes monitoring and surveillance of meta-data that can indicate an intrusion. The specific meta-data concerns server activity patterns that may indicate intrusion. Investigation of an apparent intrusion may include assessment for intrusion of individual user computers.

Wikipedia on key cybersecurity terms:

- "**Monitoring:** awareness of the state of a system, to ob serve a situation for any changes which may occur over time using a monitor or measuring devise of some sort."
- "**Surveillance:** the monitoring of the behavior, activities, or other changing information, usually of people for the pur pose of influencing, managing, directing, or protecting them."
- "**Meta-data:** are data that provides information about other data."

A group of Berkeley faculty members, responding to the installation of these security measures, as well as a lack of initial consultation from the Office of the President, raised concerns over these security measures with the systemwide Academic Senate. Subsequently, the systemwide University Committee on Academic Computing and Communications (UCCC) wrote a

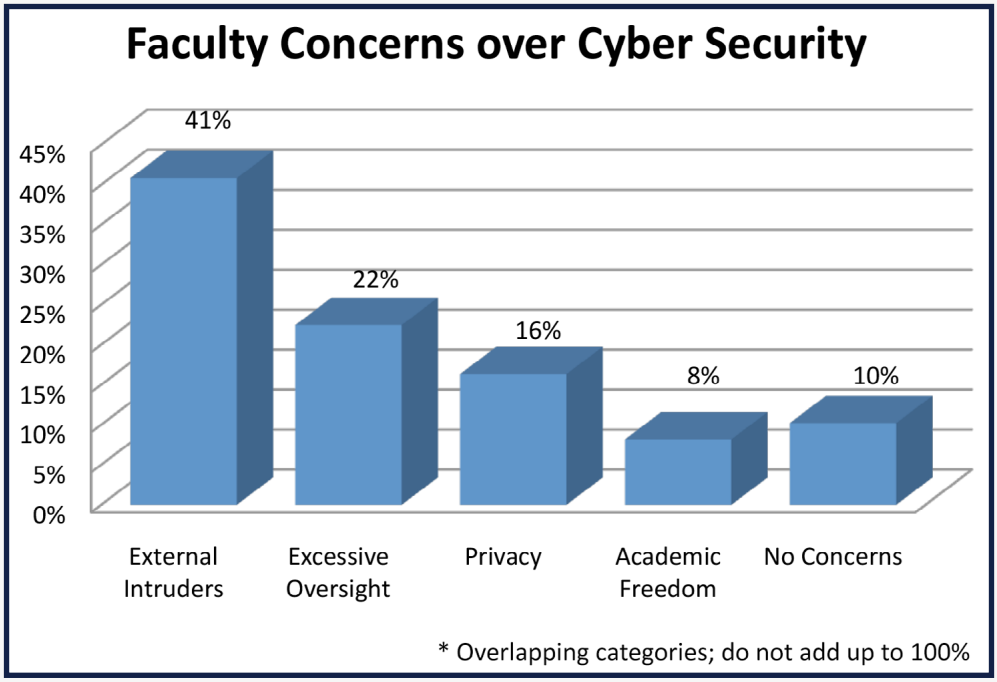
letter to the Chair of the systemwide Senate, noting that while "the faculty should have been informed and consulted at the earliest stages of the process and should be involved in future decision making, … [but recognized] that the immediate response to the UCLA cyber-attack was proportional and appropriate." UCOP also developed a systemwide website and FAQ page to better inform faculty on measures to address cyber security concerns.

As a Health Sciences campus, UCSF faculty have long realized the necessity of balancing cyber security with the pragmatic concerns over introducing so many measures that they hinder the important work and research. In a recent Question-of-the-Month, the UCSF Academic Senate asked faculty about cyber security concerns, particularly the juxtaposition of cyber security vis–à–vis privacy and academic freedom. The Senate received 49 responses to this question. In general, it can be said that faculty opinion is quite mixed and overlap concerns over external intruders, excessive oversight, privacy, and academic freedom, as noted in the chart below.

"UCSF needs to do a better job protecting our e-mail addresses, which are the first line of defense against malware. I receive >400 unwanted and unsolicited e-mails a month. Right now, a ten year old with an iPad can easily and quickly mine our e-mails."

Question of the Month: What concerns do you, as UCSF faculty, have about cyber security? Are you more concerned about external intruders, or loss of privacy to UC faculty? Are you concerned about your academic freedom? Do you think the Academic Senate should focus the June division meeting on cyber security and IT planning?

While a number of faculty responded that external intruders are a significant concern, and support measures taken to prevent such intrusions, there is a legitimate concern that too much oversight will produce unacceptable obstacles when the University engages in too much policing. Some respondents noted that past cyber security reactions have been un-even, especially in regard to email security and "one size fits all" data pushes to laptops and desktops that can sometimes lead to crashes. Indeed, the extremely mobile computing environment that UCSF faculty work in not only makes cyber security of utmost importance, but also highlights the need to customize solutions to mobile computing. In addition, charging IT-related costs to PI direct costs just because it is allowable is another concern. Indeed, in this day and age, it can be argued that such IT infrastructure costs are more akin to such indirect costs as electricity, lighting, etc.



Perhaps most surprising, of the respondents that mentioned academic freedom (24% of the total respondents), only 33% of those mentioned it as a real concern, while 67% were less concerned or not concerned

at all about the loss of academic freedom in the face of increased cyber security measures. Such a response indicates that most faculty do not feel that their academic freedom has been encroached upon to date. That said, this may be an emerging area of concern for the Senate's Committee on Academic Freedom to take up, or at least be watchful for. Privacy is another concern that largely moves in lock-step with the concerns over academic freedom. For instance, many of the respondents that were concerned about incursions into academic freedom were also concerned with the loss of privacy.

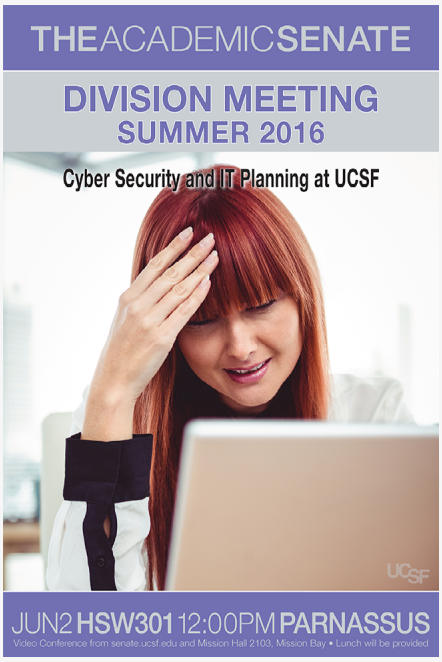
UC computer users are protected by existing privacy policies incorporated in the UC Electronic Communications Policy. Any network is operated by managers, who have always had the capacity of accessing computer content, were they intent of violating UC policy. The new cybersecurity activities do not alter this relationship.

"I agree that cyber security is necessary, but I am even more concerned about the level intrusion and the barriers placed on our ability to work freely and without concern of being monitored by the University is even more vitally important to us within the UCSF community."

It would seem that there is no absolute privacy for those who wish to use networked computers. One needs to assess the risk of intrusion by UC system managers versus outside agents. A fresh perspective on privacy might be provided by Apple, a company that recently took a very public stand for user privacy. If one lifts up the hood to examine the Apple user agreement, (a lengthy document that many users agree to with a minimal read) one finds that the user gives consent for collection of information that bears a strong resemblance to meta-data, and monitoring of activity, not to mention linkages to un-named third parties.

"Since my work is in global health, I hope to have some balance of protection while at international sites but not tremendous difficulty in accessing materials I need. Certainly from everything I see in the news, cyber security needs to be a major priority."

Overall, it can be said that cyber security is a significant concern of many UCSF faculty, as indicated by the large number of responses to the Senate's Question-of-the-Month. As such, this issue crosses a number of committees, including Academic Planning and Budget, Academic Freedom, Faculty Welfare, and the Committee on Library and Scholarly Communication. In response to these concerns, the Senate is making cyber security and IT planning a central theme of its next Division Meeting on June 2, 2016. UCSF CIO Joe Bengfort will make a presentation at the meeting, and the Senate is assembling a special panel of faculty members involved with IT planning on the campus to address questions and concerns from faculty members at the meeting.



The Summer Division meeting will be held on Thursday, June 2, 2016, from 12-2 p.m. in Room HSW-301, Parnassus, with a live video conference to MH 2103 in Mission Hall.