UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax:(510) 987-9086
http://www.ucop.edu

February 1, 2016

CHANCELLORS

Dear Colleagues:

A group of faculty members at the Berkeley campus has articulated concerns regarding some of the security measures we adopted in the wake of the UCLA cyberattack last year. The concerns focus on two primary issues: whether systemwide cyber threat detection is necessary and whether it complies with the University's Electronic Communications Policy (ECP); and why University administrators failed to publicly share information about our response to the cyberattack. The Berkeley faculty members have shared their concerns with colleagues at other campuses and with various media outlets. Unfortunately, many have been left with the impression that a secret initiative to snoop on faculty activities is underway. Nothing could be further from the truth.

I attach a letter from Executive Vice President and Chief Operating Officer Nava explaining the rationale for these security measures. As you know, leadership at all levels, including The Regents, Academic Senate leadership, and campus leadership, has been kept apprised of these matters, including through the establishment and convening of the Cyber Risk Governance Committee (CRGC). The CRGC, comprises each campus's Cyber Risk Responsible Executive (CRE), as well as a representative of the University's faculty Senate, the General Counsel, and other individuals from this office with responsibility for systemwide cybersecurity initiatives. I encourage you to share Executive Vice President Nava's letter with your faculty.

While we cannot share every detail of the actions we took in direct response to the UCLA incident (we are defending 17 class action lawsuits demanding millions of dollars of damages), or of the security measures we have instituted since that time (disclosure of details of our cybersecurity infrastructure and our readiness posture would only facilitate exploitation of identified vulnerabilities by those intent on attacking us), I have from the beginning directed my staff to make every effort to actively engage with all stakeholders and to minimize to the extent possible the amount of information that is not shared widely. I have also now asked that a website be created this week to further disseminate relevant information and developments.

In the meantime, I hope that you will convey to your local communities the following information:

1. Institutions of higher education are a prime target of cyberattacks. We create, collect, store, and use valuable information about our research and discoveries, our employees' personnel information, our students' educational records, and more. These attacks pose a serious risk to individual privacy, to the valuable intellectual property we create, and to our financial position. It is our legal and our moral responsibility as stewards of the data we maintain to protect it. When, notwithstanding our best efforts, a security incident threatens that information, we are exposed to enormous legal, financial, and reputational risk. The UCLA incident alone will cost us many millions of dollars before it is fully resolved, millions of dollars that we will not be able to invest in our research, teaching, and service mission.

2. At the system level and at every individual campus, we have subjected every proposal to enhance our ability to prevent and detect attacks to evaluation against industry standards and to analysis under the University's Electronic Communications Policy, and we are absolutely committed to doing so going forward. Also attached is a document that describes how cyber threat detection generally, and our implementation of it both in the wake of the UCLA cyberattack and going forward, is entirely consistent with the letter and the spirit of the ECP.

3. When we announced the UCLA cyberattack, we very publicly disclosed some of the measures we had taken in response, *including* engagement of a leading cybersecurity firm to actively monitor our network.

4. Personal privacy and academic freedom are paramount in everything we do. But we cannot make good on our commitment to protect individual privacy without ensuring a sound cybersecurity infrastructure. While we have absolutely no interest in the content of any individual's emails or browsing history, we must accept that active network monitoring is a critical element of a sound cybersecurity infrastructure and the interconnectedness of the University and all of its locations requires that such monitoring be coordinated centrally. Executive Vice President Nava's attached letter and description of how cyber threat detection initiatives are implemented at the University set forth in more detail the kind of monitoring that might be performed and the extraordinary efforts the University makes to avoid any intrusive measures or, when those prove absolutely necessary, to minimize them.

5. A Faculty Senate representative is and has since its inception been a member of the Cyber Risk Governance Committee. In addition, Senate members are among the industry leaders we have invited to participate on the CRGC's expert Advisory Committee, and Executive Vice President Nava and Chief Information Officer Andriola are actively engaging with the Chair and Vice Chair of the Academic Senate, the Senate's Academic Computing Committee, the Chair of the Berkeley Senate, and others.

I invite further robust discussion and debate on this topic at upcoming meetings of the CRGC and COC. In the meantime, please direct any questions to Executive Vice President Nava or to Chief Information Officer Andriola.

Yours very truly,

Janet Napolitano
President

Attachments

cc: Chairman Lozano
Executive Vice President Nava
Vice President Andriola
Chief of Staff Grossman

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

EXECUTIVE VICE PRESIDENT — CHIEF OPERATING OFFICER

OFFICE OF THE PRESIDENT
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200
510/987-0500

February 1, 2016

UC FACULTY

Dear Colleagues:

I am writing to follow up on earlier discussions about cybersecurity matters across the UC system and to share to the fullest extent possible the principles and considerations that guide the University's efforts to respond to cyber attacks.

First, I want to thank you for sharing your concerns that we maintain the privacy protections enshrined in University policy even as we significantly strengthen our cybersecurity posture. As explained below, I do not believe these imperatives conflict; in fact, they reinforce one another in crucial ways. I would like to share some key principles and practices that help ensure that privacy protections are consistently upheld in the context of network security activities, some observations about the serious cyber attack we experienced at UCLA, and information about increasingly challenging attacks that are rising at academic institutions across the country.

As you know, on July 17, 2015, UCLA publicly announced that it had suffered a serious cyber attack. The attack appears consistent with the work of an Advanced Persistent Threat actor, or APT. An APT generally emanates from an organized, highly skilled group or groups of attackers that orchestrate sustained, well-planned attacks on high-value targets. Today, much effort in the cybersecurity industry is focused on APT attacks because they are difficult to detect and highly destructive. While there is no evidence that cyber attackers actually accessed or acquired any individual's personal or medical information at UCLA, the University decided to notify stakeholders. UCLA notified 4.5 million patients about the cyber attack. Within days, several lawsuits were filed against the Regents alleging various violations of State law, all 17 of which are now pending.

The UCLA attack, while exceptional in some respects, is part of an increasing trend of cyber attacks against research universities and health care systems. Institutions of higher education are increasingly targets of APT attacks because academic research networks hold valuable data and are generally more open. Indeed, the mission of our University is to promote knowledge sharing and research collaboration, which involves responsibly sharing data. A recent report from Verizon described educational institutions as experiencing "near-pervasive infections across the majority of underlying organizations," and observed that educational institutions have, on average, more than twice the number of malware attacks than the financial and retail sectors combined.

APTs seek to illicitly harvest credentials across academic networks and then use those credentials, and the trust relationships among systems, to move laterally to other nodes in a given network. There are techniques to address such attacks, but I share these points to underscore the seriousness of the threat posed by APT attackers and the fact that, for cybersecurity purposes, a risk to what appears to be an isolated system at only one location may in some circumstances create risk across locations or units.

In recognition of these realities, President Napolitano has initiated a series of system-wide actions to strengthen the University's ability to prevent, detect, and respond to such attacks. I believe these efforts are consistent with the reasonable expectations of the University community —our students, faculty, staff, patients, research sponsors, and academic partners— that we undertake serious efforts to protect sensitive data from malicious attacks. I also believe these actions are fundamental to realizing the University's commitment to privacy. The following actions were taken:

- A leading cybersecurity firm was engaged to assist the University in responding to the cyber attack, in part by analyzing network activity at all UC locations to detect and respond to any APT activity;
- Every location submitted a 120-day cybersecurity action plan to harden systems and improve administrative and physical safeguards;
- A Cyber-Risk Governance Committee (CRGC) was established, with representation from across the system, including the Academic Senate, to oversee and guide system-wide strategies and plans related to cybersecurity. The CRGC has met several times already and is identifying key ways to strengthen our security posture while honoring the University's commitment to academic freedom, privacy, and responsible fiscal stewardship;
- A system-wide incident escalation protocol was developed to ensure that the appropriate governing authorities are informed in a timely way of major incidents; and
- Mandatory cybersecurity training was rolled out to all UC employees by October 1, 2015.

Several faculty members have requested detailed, technical information about the UCLA attack and the specific security measures taken in its immediate aftermath. I understand that some are concerned that such measures may have exceeded the University's policies governing privacy. I believe such actions were well within the operational authority of the University and in alignment with policy. It is regrettable that as long as the UCLA incident remains the subject of pending legal matters, I cannot publicly share additional information that might correct some of these misimpressions. As a policy matter, however, I wish to address the privacy and governance concerns that arise in the context of data security, without any express or implied reference to the UCLA attack.

With respect to privacy, the letter and structure of the University's Electronic Communications Policy (ECP) reflect the principle that privacy perishes in the absence of security. While the ECP establishes an expectation of privacy in an individual's electronic communications transmitted using University systems, it tempers this expectation with the recognition that privacy requires a reasonable level of security to protect sensitive data from unauthorized access. For this reason, the ECP expressly permits routine analysis of network activity "for the purpose of ensuring reliability and security of University electronic communications resources and services." (ECP, IV.C.2.b.) It expressly permits analysis of "network traffic" to "confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network." (ECP, V.B.) Significantly, "consent is *not required* for these routine monitoring practices." (Emphasis added.) In short, the ECP reflects that, in some circumstances, the protection of privacy actually *requires* limited examination of electronic communications. (ECP, Attachment 1, V.A (noting that failure to prevent unauthorized access itself undermines privacy and confidentiality).) This is consistent with fair information practice principles and the University's duties under laws and regulations that require the use of physical, technical, and administrative safeguards to secure sensitive information.

The University takes great care to ensure that its practices reflect the balance outlined in the ECP. I would like to illustrate significant measures that we undertake to honor privacy rights in responding to a cybersecurity threat.

Even in time-sensitive circumstances, privacy impacts are typically evaluated before undertaking a coordinated network security effort. Appropriate privacy protection measures are embedded into the underlying scope of work both at the planning and execution stages of a network security effort. Such analysis typically includes an evaluation of the specific technical and analytic techniques to be used and whether they are consistent with the ECP. It also often means defining an appropriately limited scope for network analysis activity, focusing such analysis on known signatures for APT activity and related indicators of compromise. For vendors, the ECP requires scope discipline to be enforced by contract. (*See* ECP, IV.A (requiring vendors to be contractually bound to honor University policy).)

Layered review is another privacy-enhancing measure used in appropriate circumstances.[1] Layered review requires security alerts to be resolved in tiers, with each tier representing a limit on the type and amount of data to be reviewed. A layered review starts at the lowest tier, using automated review and basic metadata to resolve the security alert at that level. In circumstances where a security threat cannot be resolved at a lower tier or with automated means alone, the human-readable content of an underlying communication may be reviewed. The ECP limits such inspection to the "least perusal" necessary to resolve the concern. (ECP, IV.C.2.b & V.B.) To inspect content beyond what can be examined through "least perusal," the ECP requires user consent or access without consent under a campus's procedures, which typically involves a decision from the campus's senior management.

[1] A layered review is not actually required by the ECP and may not be appropriate in all cases, but it illustrates the types of measures used to rigorously observe privacy principles.

I understand that some faculty members may be concerned about storage and use of data collected through network security analysis, including questions about data being used by the University for other, unrelated purposes. The ECP forbids the University from using such data for non-security purposes, (ECP, II.E.2, IV.A, & IV.C.2.b (prohibiting University employees from seeking out, using, or disclosing personal data observed in the course of performing university network security duties)), and violators are subject to discipline.[2] With respect to storage, much data collected through network analysis may already be stored elsewhere within the University's network ecosystem (or even with third party cloud or other providers), independent of any network analysis activity. Data collected or aggregated specifically for network security purposes is only stored for a limited time, segregated in a highly secure system, and forensically obliterated thereafter. In some circumstances, a preservation of certain data related to litigation may be required by law, which may result in a longer storage period for a limited amount of network analysis data subject to such a mandate. With respect to third party requests for such data, the University has a long history of defending against improperly intrusive requests, including requests under the Public Records Act.[3]

Governance is also a critical aspect of this discussion. Ensuring that all stakeholders are fully enrolled in developing the University's cybersecurity policies going forward is essential. As you know, the President has launched a coordinated system-wide initiative to ensure that responsible UC authorities are appropriately informed about risks, that locations act in a consistent and coordinated way across the entire institution, and that the University can sustain action to manage cyber-risk. A number of structures have been put in place to elevate the importance of cybersecurity within University governance, some of which I described above but elaborate here for emphasis:

- The President asked the Chancellors to each appoint a single executive to lead efforts to review and improve cybersecurity at their location. These positions are the Cyber-Risk Responsible Executives (CREs), and each position reports directly to the Chancellor or location chief officer.
- A single escalation protocol has been implemented across the UC system to facilitate appropriate notification and handling of cybersecurity incidents. The protocol is intended to drive consistent analysis and response to cybersecurity incidents. It is being piloted and will be reviewed for effectiveness by the CRGC after six months.
- In addition to establishing the CRGC described above, the President has appointed a Cyber-Risk Advisory Board, composed of six internal and external expert advisors, to support the CRGC and provide information and advice about emerging issues and best practices in cybersecurity, and to help develop aggressive and effective approaches to managing cyber-risk, consistent with UC's teaching, research, and public service mission.
- Finally, a Cyber Coordination Center is being launched to help coordinate a variety of activities across the locations.

[2] The ECP creates a specific exception for circumstances where an employee incidentally observes obvious illegal activity in the course of performing routine network security activities. (ECP, IV.C.2.b (defining exception for disclosure of incidentally viewed evidence of illegal conduct or improper governmental activity).)

[3] Public Records Act requesters may seek far more intrusive access to the content of faculty or staff records than what the ECP permits for network security monitoring. The limits on the University's own access to electronic communications under the ECP do not apply to Public Records Act requests.

With specific reference to faculty governance, the President has reinforced with senior management the need for ongoing dialogue with our faculty and Senate leadership. The Senate has a robust presence at the CRGC, and I believe the CRGC is the best forum to develop mechanisms and policies for further ensuring that Senate leadership is fully engaged in policy development and briefed in a timely way regarding ongoing security matters and practices.

I also welcome a discussion about how to harmonize broader cybersecurity efforts with existing, campus-specific information governance guidelines. Some campus-level guidelines, established as part of system-wide information governance initiatives, limit the specific technologies and methods that may be used for network security activities, including some methods in ordinary use at other University locations and use of which may be necessary to comply with legal duties or to effectively evaluate a specific threat that may implicate multiple locations.

Given the difficult and shifting challenges worldwide in terms of cybersecurity, there is no monopoly on wisdom here. It is my intention to approach these issues with humility and openness, believing that our efforts will only be enriched by an exchange of ideas and viewpoints. I welcome your engagement on these issues and look forward to a deeper, joint effort to protect the privacy of our users and the security of the University's systems.

Sincerely,

Rachael Nava

Rachael Nava
Executive Vice President - Chief Operating Officer

cc: Chancellors

Network Security Activities Under the University's Electronic Communications Policy

This guidance is intended to assist the Campuses and Laboratories in undertaking additional network security efforts. This guidance specifically addresses how the University's Electronic Communications Policy (ECP) applies to network security activities. Because technology develops so much more rapidly than policy, this guidance is limited to describing the basic principles of the ECP and how they apply to general categories of network security activities. For more specific advice with respect to a particular network security technique or functionality, Campuses and Laboratories are encouraged to consult with their respective Cyber-Risk Responsible Executive and/or the Office of General Counsel.

I. General Rule: Access to Electronic Communications Requires Consent

The ECP establishes the following general rule: "An electronic communications holder's consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications records in the holder's possession." This basic rule establishes the default expectation of informational privacy for authorized users of the University's electronic information systems.

II. Exceptions to the General Rule: System Monitoring and Security Practices

The ECP expressly authorizes network security activities, including inspection of network traffic for security purposes:

> University employees who operate and support electronic communications resources *regularly monitor transmissions for the purpose of ensuring reliability and security of University electronic communications resources and services* (see Section V.B, Security Practices), and in that process *might observe certain transactional information or the contents of electronic communications.* Except as provided elsewhere in this Policy or by law, they are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed. In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) *shall be limited to the least invasive degree of inspection required to perform such duties.*

(ECP, Section IV.C.2.b (emphasis added).)

The System Monitoring authorization is supported by an additional provision of the ECP that includes express authorization for "Security Practices":

> Providers of electronic communications services ensure the integrity and reliability of systems under their control through

> the use of *various techniques* that include routine monitoring of electronic communications. *Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation. User consent is not required for these routine monitoring practices.* Providers shall document and make available to their users general information about these monitoring practices. If providers determine that it is necessary to examine suspect electronic communications records beyond routine practices, the user's consent shall be sought. If circumstances prevent prior consent, notification procedures described in Section IV.B.3, Notification shall be followed.

(ECP, Section V.B).

Like the "System Monitoring" provision, the "Security Practices" provision contemplates that network security monitoring may include access to contents of communications, following the "least perusal" principle.

This provision also requires that general information should be made available to users about the University's network security practices. This does not require the dissemination of technical details or specific functionalities. The purpose of this provision is to provide "general" information about such activities, in clear terms that are understandable to users who may not have technical expertise.

a. Use of Automated Systems for Network Security

The ECP's Implementation Guidelines explicitly provide that "automated inspection of electronic communications in order to protect the integrity and reliability of University electronic communications resources does not constitute nonconsensual access." (ECP, Implementation Guidelines Section III.B.4.) Some basic network security tools, such as intrusion detection systems, use automated technical features to identify potentially malicious activity on a campus or location's network. The ECP specifically exempts such automated inspection techniques from the consent requirement to protect the integrity and reliability of the University's systems.

III. Limits on System Monitoring and Security Practices

The ECP permits review of both the transactional elements and the content of electronic communications to respond to a network security threat. To protect the privacy of users, the ECP also imposes important limitations on such review.

a. "Least Perusal" Standard

The inspection of network traffic for security purposes must be limited to "least perusal of contents required to resolve the situation." (ECP, IV.C.2.b & V.B.) This means, for example, that a Campus or Laboratory should attempt to resolve a security concern by review of transactional data at first, without review of the human readable content of an underlying electronic communication.

In circumstances where a security threat cannot be resolved at a lower tier (or, indeed, where security concerns are *amplified* by such review of transactional data), the human-readable content of an underlying communication may be reviewed. In such cases, the ECP limits such inspection to the "least perusal" of content necessary to resolve the concern. To inspect content further than is permitted for routine network security purposes, the ECP requires user consent, or access without consent under a campus's procedures, which typically involves approval by Campus or Laboratory's upper management, as discussed below.

b. Restrictions on Use of Network Security Data

The ECP forbids the University from using network security data for non-security purposes, (ECP, II.E.2, IV.A, & IV.C.2.b (prohibiting University employees from seeking out, using, or disclosing personal data observed in the course of performing university network security duties)), and violators are subject to discipline. The ECP does create a specific exception for circumstances where an employee incidentally observes obvious illegal activity in the course of performing routine network security activities. (ECP, IV.C.2.b (defining exception for disclosure of incidentally viewed evidence of illegal conduct or improper governmental activity).)

With respect to storage, much data analyzed through network analysis may already be stored elsewhere within the University's network ecosystem (or even with third party cloud or other providers), independent of any network analysis activity. Data analyzed or aggregated specifically for network security purposes should only be stored for a limited time, segregated from other network resources in a highly secure system, and forensically obliterated thereafter. In some circumstances, a preservation of certain data related, for example, to anticipated litigation or a regulatory investigation, may be required by law, which may result in a longer storage period for a limited amount of network analysis data subject to such a mandate. With respect to third party requests for such data, the University should carefully scrutinize such requests, from whatever source, to ensure that user privacy expectations are protected.

c. Vendors and Contractors Performing Network Security Activities

For vendors who assist with network security activities, the ECP requires them to be contractually bound to honor University policy, including the ECP. (*See* ECP, IV.A.) It is also recommended that, even in otherwise time-sensitive circumstances, privacy impacts should be evaluated before undertaking a coordinated network security effort. Appropriate privacy protection measures should be embedded, as feasible, into the underlying scope of work both at the planning and execution stages of a network security project. Such analysis typically should include an evaluation of the specific technical and analytic techniques to be used and whether they are consistent with the ECP. Campus and Laboratory security and IT teams may properly consult with their respective privacy officials and the Office of General Counsel to assist with such analysis, including defining an appropriately limited scope for network analysis activity. To further ensure adherence to University policy, it is recommended that vendors agree to follow the ECP and the University's standard terms and conditions related to data security, currently contained in Appendix DS.

IV. Access Without Consent (AWOC)

In addition to the broad exception to the consent requirement for network monitoring and security practices, additional exceptions provide for review of the content of electronic communications: when required by law, when there is substantiated reason to believe violations of law or certain University policies have taken place, when there are compelling circumstances, and under time dependent, critical operational circumstances. Where one of these exceptions apply, the policy authorizes the University to obtain authorization to review from an official designated by campus policy under the "Access Without Consent" or "AWOC" provisions of the ECP and may require notice to an affected individual rather than consent. (ECP Section IV.B.) Each campus has designated an approving official at a senior level.

###