Committee on Data, Information Technology and Privacy

Recommendations Around FireEye Endpoint Security

Table of Contents

Generated 9/28/2022 8:57 PM

UCLA Academic Senate
Executive Board

May 31, 2022

Lucy Avetisyan
Associate Vice Chancellor/CIO

Re: **Recommendations around FireEye Endpoint Security**

Dear AVC/CIO Avetisyan,

At its meeting on May 12, 2022, the Executive Board reviewed the attached letter from the Committee on Data, Information Technology, and Privacy (CDITP) about potential recommendations around FireEye Endpoint Security.

Members of the Executive Board unanimously endorsed the letter, and pointed to CDITP as the logical Senate body to work with Administration on its recommendations.

We would appreciate a response regarding the enclosed recommendations.

Sincerely,

Jessica Cattelino
Chair
UCLA Academic Senate

Encl.

Cc: Michael Beck, Administrative Vice Chancellor
April de Stefano, Executive Director, UCLA Academic Senate
Andrea Kasko, Vice Chair/Chair Elect, UCLA Academic Senate
Michael Levine, Interim Executive Vice Chancellor and Provost
Emily Rose, Assistant Provost and Chief of Staff to the EVCP
Shane White, Immediate Past Chair, UCLA Academic Senate

UCLA Academic Senate

Committee on Data, Information Technology, and Privacy

May 5, 2022

To: Jessica Cattelino, Chair
Academic Senate

From: Alex Bui, Chair
Committee on Data, Information Technology and Privacy

Re: Potential Recommendations Around FireEye Endpoint Security

Dear Chair Cattelino and Executive Board Members:

As many of us are aware, there has been heighted awareness and concern regarding the deployment of FireEye Endpoint Security (FES) software from UCLA's Information Technology Services (ITS). We are writing to provide some context, observations about the issues surrounding its rollout, and to suggest a path forward addressing our colleagues' concerns. What we write is informed based on emails that have been shared with us regarding faculty concerns around privacy and shared governance; our attendance at different faculty meetings; discussion at the Committee on Data, Information Technology, and Privacy (CDITP); and interactions with campus IT leadership.

Executive Summary

- Reasons for FES. FES is antivirus/malware protection software. A UC-wide agreement was made for FES after a ransomware attack at another UC campus, with UCOP covering the costs for any campus implementing it. It is presently implemented, in different ways, at other UC campuses. The use of FES helps address UCOP's IS-3 policy, which governs the protection of all electronic data.
- Faculty concerns. Faculty have raised many concerns about FES, which fall into three categories: 1) questions around **privacy and data access**, especially when sensitive and/or personal information are involved, and apparent new abilities by the administration to view such data without permission; 2) questions about **impact on older or specialized computers**; and 3) questions around **IT shared governance**, and how the *decision* to implement FES on this campus was made.
- Response to FES rollout. A combination of factors, including misinformation; lack of effective communication; distrust of ITS; and continued absence of shared governance in decision-making has resulted in several departments and groups on the campus deciding not to install FES. ITS has responded to some issues, yet there remain significant gaps. Multiple issues have combined that highlight IT governance problems.
- Takeaway from the FES rollout. Communication around FES was key to the success at other UC sites, and so the lack of transparency and ineffective communication by our ITS has been problematic. This rollout is seen as an exemplar of the lack of shared IT governance and other issues. There are clear opportunities for better education of our faculty around existing campus IT procedures/policies – including those that protect their

rights. There is also a clear need for determining what procedures are followed for any IT-related approval, and jurisdictional purview and responsibilities of all stakeholders.

UCLA's historical commitment to privacy appears to be at risk. **Our own UCLA faculty helped craft IS-3, yet its implementation now is in the absence of its intent.** We believe this was not the intent of the administration. CDITP's has three recommendations to address several concerns about FES:

1. Reaffirm UCLA's commitment to privacy and data protection. UCLA has existing policies and procedures in place around data access (e.g., Policy 410), yet our Academic Senate faculty and staff are unaware of these. All stakeholders – ITS, Administration, and Academic Senate leadership, should recapitulate a commitment to these ideals and existing processes.
2. Reassess communication about FES. Existing resources published by ITS (e.g., the frequently asked questions, FAQ, page) are not helpful to faculty. These need to be (re)written in a way that address faculty concerns in an effective manner. Overall communication around FES needs to be improved.
3. Transparency around FES usage. Appoint an Academic Senate group to oversee regular data accesses, particularly from FES, ensuring that appropriate methods are in place around privileged access. This information should be published regularly for all faculty to see.

FireEye Endpoint Security Summary Report

Context. University of California (UC) campuses have suffered several recent data breaches, including a well-known ransomware attack at UCSF that resulted in costs of over $1M to recover a researcher's data. Recognizing the need to better protect electronic infrastructure, UC Office of the President (UCOP) and each campus have taken steps to address these issues. A few key points below provide a bit of the backdrop for our current situation:

1. UC Policy IS-3 (*Electronic Information Security*) governs how all UC campuses and medical centers must handle and protect data, particularly safeguarding privacy and for the institution to meet legal and regulatory requirements. Of note, given several large-scale data breaches that have occurred on UC campuses in the past couple years, UCOP has asked an independent group to conduct audits of every campus' infrastructure around IS-3, making recommendations and noting potential points of network vulnerability. This group, which reports directly to the UC Regents, can only make recommendations, leaving mitigation and resolution of identified problems up to each campus.
2. UCOP made a UC-wide agreement for FES software, covering costs for any campus that uses it.
    a. Several other UC campuses are using FES across their systems or mix of systems. The sites we are aware of include UC Davis, Berkeley, and Santa Barbara.
    b. At UCLA Health, decisions were made to install FES on all machines operated by Health System's IT group, Information Systems and Solutions (ISS). As a result, all faculty members in DGSOM have this software installed on: 1) devices purchased by the university; and 2) must have installed on an machine that connects via virtual private network (VPN) into the Health System, including *personal devices*. As such, *it should be noted that ISS' policy is more stringent than the current UCLA campus requirement that is limited to only UCLA-purchased devices.*
    c. UCLA main campus, in response to IS-3, determined that it needed to have better software in place to protect against external intrusions. It also decided to go with FES. By the estimates described by administration, for UCLA this reflects probably a saving of $200,000/year. Note that cost savings were not the only consideration in choosing FES, as it was assessed by ITS to be a superior product over others to provide timely response in cases of data security breach.
    d. The description of FES is given here: https://www.ociso.ucla.edu/services/fireeye-endpoint-security-antivirus. FES is presented as antivirus software and is the replacement for the well-known Sophos software that the campus supported.
    e. FES is not necessarily a permanent solution. While FES is being renewed for another year by UCOP, there is a planned request for proposals (RFP) that will assess its usage. Notably, faculty will be part of the planning for threat detection and identification methods: the RFP from UCOP is forthcoming and will be (hopefully) sensitive to faculty concerns across campuses.

Markedly, the campus decision to use FES, so far as we are aware, was not one of shared governance. While it was presented to various faculty groups, including CDITP, the decision process was presented as *fait accompli*. Arguably, this also happened during a challenging time – during COVID-19 response, as well as during the start of a new campus Chief Information Officer (CIO) position addressing multiple issues (after the campus had no CIO for an extended period).

Current situation. Unfortunately, the deployment of FES by ITS has been problematic and suffered from a lack of communication, as well as other major issues, with our UCLA faculty and staff. The lack of useful and timely information – alongside other IT initiatives that have affected faculty in the past year – have engendered significant mistrust. Sharply divided visions about centralized IT and academic freedom (as far as an individual's governance over their individual devices) have arisen, especially given FES. While several departments have already installed the software, more recently, other departments and groups from the social sciences and humanities have voiced many concerns and have voted *not* to install the software. Multiple issues have been

cited, largely around the software's capabilities and potential intrusion into academic freedom and privacy. Broadly, the concerns fall into three categories:

1. The software (and hence administration) will have access to my computer, including any sensitive or private files. While the university already has access to email, access to hard drives is perceived as a new ability. Furthermore, it is unclear whether the university could directly access files like research data about sensitive issues when facing a public records request or subpoena.
2. The software will adversely impact the performance of different systems, including high-performance computing and older computers.
3. This action further represents the centralization of IT and my computer system should not be under mandate/control by the administration.

All the above concerns are valid and should be addressed, allaying fears about privacy and related computational infrastructure (see below for potential solutions). To ITS' credit, we note a few things:

- ITS leadership, including Lucy Avetisyan (CIO) and David Shaw (Chief Information Security Officer, CISO) have been presenting to faculty in different settings, including CDITP, the Institute for Digital Research and Education (IDRE) Executive Board, and departmental/School townhalls.
- ITS has set up a frequently asked questions (FAQ) webpage: https://www.ociso.ucla.edu/services/fireeye-endpoint-security-antivirus/faqs to answer commonly received questions.
- ITS has set up an exception process whereby different machines can be exempted from the installation of the FireEye software.
- The CISO has committed previously to allowing any IT group to review the logs and information captured by FES, in assuring full transparency around the process. However, as noted by some faculty, this has no faculty involvement.
- FES has *worked as promised at UCLA*. Per ITS, it has already stopped a ransomware attack akin to that seen by UCSF. While this was not made widely known to our campus, it demonstrates the need for appropriate tools to be in place to safeguard our campus' digital assets.

Still, there is also a deeper question being surfaced in the faculty's response to FES and other IT initiatives. We have no specific policies or guidance around emergent issues and IT infrastructure as a matter of shared governance, or of what elements faculty vs. administration will be responsible for. There are also downstream questions about policy and procedure around FES. Consider the following hypothetical scenario: say Group A at UCLA decides not to install security software while Group B, also at UCLA does – and Group A is "hacked" with a ransomware attack – who should pay? Per the UCSF example, the campus/Regents paid to recover the data. If the attack could be prevented by software, then should we hold Group A specifically responsible to cover the associated costs? *Already, there are real-world ramifications of such scenarios, as cybersecurity insurance will be dependent on some basic level of compliance to security measures* (i.e., the insurance purchased by the campus or UC will be dependent on our ability to demonstrate that we are taking measures that are effective to protect against attacks). These issues must be balanced and understood by all stakeholders, including the faculty. Open discussion and communication around these issues is critical so we can work together to address these problems.

Potential solutions and moving forward. The above presents a complex set of topics, and our goal is to suggest a few ways in which we can address the immediate concerns of faculty. Undoubtedly, communication is key, and brief discussions with colleagues at other UC sites that implemented FireEye noted the same concerns being raised by faculty, but these issues were ameliorated through active communication and transparency by their IT leadership and staff in a proactive manner. While we may be somewhat beyond that point at UCLA, there are several recommendations and positive actions we can take.

Regarding the question of software access. As presented by UCLA, FES "only" has access to operating system data logs on one's hard drive, while some faculty point to the fact that it can indeed access specific files. The

response in this case has been unclear: yes, it can "grab" a specific file, but only if the specific file location and details are known. Unfortunately, this does not alleviate the concerns many faculty may have on sensitive data being collected, especially without their knowledge or consent. Two points:

1. The CISO and ITS have noted that it is their procedure to follow 1 of 2 paths for accessing any data. The first option is to ask the owner of the computer/file for permission to access it. In the case the individual declines or is unavailable, then a non-consensual access procedure is invoked (Policy 410), which requires signoff by multiple parties include the leadership of the Academic Senate. These processes are longstanding at UCLA – but they are not known by our faculty. We and the administration should: 1) educate our faculty about these processes; and 2) ensure that the administration will uphold these processes. *Markedly, several faculty and staff have raised red flags about different reasons for access (e.g., subpoenas, Freedom of Information Acts, other legal inquiries) that may "subvert" the process or that ITS would not follow*. For this reason, **it would be important to make clear and reaffirm the policies and procedures that will govern data access processes.**
2. **The FAQ should be rewritten to be more conducive to faculty and staff concerns**. It is presented as a technical brief, rather than helping the faculty (and others) understand and address concerns.
3. It was recommended that **a regular body/entity be set up to review the FES data access logs and who (from ITS and other associated groups) access any data**. For example, regular (e.g., quarterly) reports from ITS to CDITP or some other Academic Senate body (e.g., Executive Board, a select faculty group, etc.) to review all cases in which FES found issues and then data was accessed may assure our faculty that no improper access has occurred.
    a. It may also be useful, for example, to **publish "dummy" logs of the data that are accessed by FES** so faculty and staff understand what is being "shared" by default and then create assurances, per the above, about file access. Discussion about access has occurred, to date, in the abstract.
    b. It may also be helpful to **understand other situations in which FES has worked**, as promised. Information could also be presented from UCLA Health.
    c. We **(Academic Senate) should publish and share reports around FES on a regular basis (perhaps annually**).

Relative to 3b, we believe many DGSOM faculty would also welcome some "disentanglement" in this regard. For example, many of them are part of the Academic Senate, yet their FES data is not seen by campus and instead only by UCLA Health. **How these individuals' data are "accessed" should be in a manner similar to that of main campus relative to academic freedom and privileges (arguably)**. Should there be subsequent "segregation" of users based on context, then an appropriate method to handle these issues should be considered before implementation.

Regarding impacted computational systems. We believe that ITS has done its due diligence in this area, setting up an exception process that considers risk vs. benefit appropriately. The process, as described thus far, has been easy and straightforward, with multiple levels of assessment and consideration. One suggestion, which was raised recently in discussions, was whether **the installation of FES be considered only on new machines, rather than being installed on older, existing machines – such a policy moving forward may be useful to mitigate some concerns. Additional ways of thinking about opt-out should be considered and formalized, too.**

Regarding IT communications and shared governance. While CDITP has suggested over the past year an increased need for communication by ITS to faculty, and there has been some effort in this regard, we would highly **suggest a concerted effort to engage with the faculty**. Specifically, around FES, we recommend **rewriting the existing FAQ** (per above). As it stands, the information is buried deep in the page, presenting it from a technical perspective rather than one of a faculty member who has concerns. We also note a concern about *which* parties should be interpreting IS-3 policies. **Our own UCLA faculty helped to craft IS-3, yet its implementation now is in the absence of its intent**.

Summary. Hopefully we have managed to provide both context around the discussion of FireEye and provided some context to move forward with recommendations that the Executive Board can utilize. We recognize that several of the concerns raised by faculty around FES are notable, yet there is also some misinformation that needs to be addressed – if not deeper issues. Regardless, we hope the campus can move forward in a constructive manner around it and welcome feedback from the Executive Board as well as recommended actions for CDITP based on this report.

Thank you for the opportunity to provide the above recommendations. If you have any questions, please do not hesitate to contact buia@mii.ucla.edu. or the Committee Analyst, at rrouzankay@senate.ucla.edu.

cc: Shane White, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Renee Rouzan-Kay, Committee Analyst, Academic Senate
Members of the Committee on Data, Information Technology and Privacy