UC SANTA BARBARA
THE Current

February 11, 2025
Nora Drake

Raising the bar on cybersecurity: Q&A with Jackson Muhirwe and Shea Lovan

In the past five years, cybersecurity threats to UC Santa Barbara have increased more than tenfold. While the university faces a persistent and evolving landscape of threats, costly cybersecurity incidents and data breaches affect everyone on campus.

To mitigate some of these incidents, President Michael Drake instructed each UC campus to prepare a comprehensive cybersecurity investment plan, to be implemented by May 2025. At UC Santa Barbara, that plan is called Secure UCSB.

With Secure UCSB now being rolled out, Jackson Muhirwe, Chief Information Security Officer and Shea Lovan, Chief Technology Officer, answered some questions about the plan and what it means for the campus.

Q: What are the components of the Secure UCSB plan?

JM: There are three focus areas: network equipment upgrades, device security implementation and training compliance.

SL: The network upgrades are the first step in meeting the vulnerability management portion of President Drake's memo. Between now and summer 2025, we will replace over 1,000 devices in over 400 buildings. Unfortunately, this work

requires network service outages in virtually every part of the UCSB campus. In most cases, people will experience two outages lasting one to two hours, but in some cases, they will take longer. Departments will receive notifications of any outages at least 14 days in advance, and they will also receive informational flyers they can print to share the news with building occupants.

After the network equipment has been upgraded, we will simplify the campus network while improving the security of our community. This will also improve the reliability and performance of UCSB's campus network.

JM: Yes, and for device security implementation, anyone who has a UCSB-issued device (computer, tablet, phone, etc.) will be required to install threat detection and response software called Trellix. This will be installed via a device management (MDM) platform called either Maas360 or Jamf, depending on your operating system. Trellix will detect cyber threats and malware, and identify and fix vulnerabilities. MDM software ensures your devices can be accessed remotely, should they be lost, stolen or otherwise compromised in a security incident.

For training compliance, all UCSB employees are already required to take an annual cybersecurity awareness training course. The new mandate means that UCSB will begin enforcing training compliance in order to meet the UCOP mandate's requirement of 100% compliance. All faculty, staff and student employees **must** complete the 35-minute training by April 30, or risk losing access to important systems like Canvas, Google Suite and Zoom.

Q: How do I know when my building will have an outage?

SL: The next six weeks of outages are listed here. I recommend checking this link regularly and also being alert to any notifications that come through email. As I mentioned, we will be emailing department and building managers, and they are likely to share these notifications widely with office occupants.

Q: If I don't see my building on the list of upcoming outages, does that mean it isn't scheduled?

SL: Not necessarily. We are only publishing buildings scheduled six weeks out as we continue to finalize later outage dates. This could also mean that your building is already upgraded. We encourage you to review the Completed Buildings page to see if a building has already gone through the necessary updates.

Q: Could you clarify what sort of devices will need to be running the security software?

JM: The mandate applies to any UCSB-owned device that is connected to any network with external connectivity (including remote employees) and is capable of running the software. These devices might include computers, tablets or phones that were purchased on behalf of an employee or using research funds.

Devices running older operating systems not supported by the MDM or EDR solutions should be upgraded if possible. If operating system and/or hardware upgrades are unable to be performed, the devices will need to go through the exemption process, which includes identifying alternate ways to ensure their security.

Q: Do users need to do anything to get this new MDM software installed? Will it change the way our computers run?

JM: Your Local IT unit will be responsible for deploying the software on your devices. Please be on the lookout for communications for them about how they will install it. In some cases, it can be installed remotely with no impact to your daily work. Others may need to schedule installation.

Nothing about the experience of using your devices should change with this implementation. The UCSB Security Operations team has worked with several research-oriented departments at UCSB to troubleshoot and resolve any performance issues that were caused by initial tests of Trellix. Should any issues arise, the team has outlined procedures to work with Departmental IT staff to troubleshoot, identify and resolve them.

Q: I use my personal device for work a lot. Does it need to have software installed on it?

JM: Not at this time. We are exploring lower-impact solutions for personally-owned devices on campus (Bring Your Own Device or "BYOD").

Q: I value my privacy. Will UCSB be using this software to access my device without my knowledge?

JM: No. We value your privacy, too. All tools deployed by Secure UCSB must be in compliance with UCSB privacy policies and guidelines, including the UC Statement of

Privacy.

This is especially important for users to understand: enrolling a UCSB-owned device to the needed cybersecurity tools **does not** equate to providing access to your local (personal or UCSB related) files, emails, browsing history, or any other standard, activity-related information. The tools focus on collecting relevant information to determine if the devices are vulnerable to cyber threats. I encourage everyone to read more about privacy considerations here.

Q: How do I know if my Cybersecurity training is current?

JM: You can log in to SumTotal, UCSB's learning management system to check the status of your UC Cyber Security Awareness Fundamentals training. If you are up-to-date on this training, it will say "Attended" in green text at the top of the page.

Q: What will happen if I miss the deadline and don't do the Cybersecurity Awareness training?

JM: Before you miss the training, we will send you both email and popup browser warnings, starting 30 days from expiration date. If you still don't take the training and your credential expires, you will be redirected to SumTotal to take the training when you try to log in to an application that uses Single Sign On (SSO)--like Gmail, Zoom, or Canvas. Once you have completed the training, you will regain access to log in through SSO.

Q: This is a lot of change happening at once. What's the bigger picture? Why does it matter?

JM: Besides the fact that we want to comply with President Drake's mandate, I like to remind people that the cybersecurity fight is both institutional and personal. Even I, the Chief Information Security Officer for UCSB, have had my personal information compromised by a data breach. We all have. When a breach happens, there's no discrimination. Everyone gets impacted. So, while I know we all wish that we had a little more time to make these changes, if we take a step back and think about it as a little temporary discomfort for greatly enhanced security that will benefit us all, I believe it's worth it.

Media Contact
Nora Drake

Communications Manager
Information Technology Services
Office: 805-893-2206
noradrake@ucsb.edu

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.