

**UC Tech Awards 2023 Candidate**

**Category: UC-WIDE COLLABORATION**
**Name:** Covering two locations with one CISO: Patrick Phelan (4)
**Number of people** (4)
**Location:** UCSF and UC Davis

1. **Person submitting the application/nomination**
	1. **Name, title, department, location/organization, and please indicate if you are faculty or staff:** Patrick Phelan
	2. **Email address:** patrick.phelan@ucsf.edu
	3. **The name of your organization:** UCSF
2. **Award category** UC-Wide Collaboration
3. **Name of person, name of the team, or name of the project to receive the award** Patrick Phelan, Chief Information Security Officer, UCSF

NB: Laurel created a possible alternative title for the project: “Covering two locations with one CISO”

1. **All project team members - if applicable**
2. Patrick Phelan, Chief Information Security Officer, UCSF
3. Lee Smith, Security Operations Manager, UCD Health
4. Scott Harrison, Chief Technology Officer, UCD Health
5. Ashish Atreja, Chief Information Officer, UCD Health
6. Joe Bengfort, Chief Information Officer, UCSF
7. **Which location was affected by the work?** (the name(s) of the organization affected)

UCSF and UC Davis Health

1. **Summary** Through effective collaboration at several levels, UCSF and UC Davis Health shared a single Chief Information Security Officer for two years. The arrangement benefited both organizations in form of duplication of successful programs and cost-savings through improved negotiating leverage and reduced labor.

*[Note: I prepared this nomination last year but missed the deadline due to COVID. Yvonne suggested I submit this year.]*

1. **Narrative**

There is a critical talent shortage in the cybersecurity field. Attracting and retaining qualified workers has grown progressively more difficult over the last decade. Recent research conducted by CyberSeek, a government-funded program established to address the issue, found that there are only 68 qualified workers available for every 100 cybersecurity jobs.

When UC Davis Health (UCDH) had difficulty recruiting for its vacant CISO role, leaders approached UCSF to discuss the possibility of having one CISO cover both locations. The approach would enable UCDH to fill the CISO role with a qualified candidate, one familiar with the extraordinary complexity of the UC Health system, align security strategy across two locations with similar risk profiles, and share expertise, all while achieving cost savings. In August 2019, in addition to my CISO duties at UCSF, I became CISO of UCDH, a role I would keep until December 2021.

Over the course of the nearly two and a half year-experiment, we accomplished our initial goals and more. With the support of the security team, Patrick and Lee were able to improve security program maturity significantly, as measured by Cynergistek, a third-party firm we use to assess our program against a commonly used cybersecurity framework. Some of the key accomplishments borne of the shared-CISO relationship:

* Patrick and Lee established regular communication about cybersecurity with UCDH executive leadership, including the CEO and Deans. Prior to this, there was limited interaction between the business and IT security.
* We were able to duplicate approaches and reuse documentation for three key major security services provided at each location using the same products: data loss prevention (DLP), vulnerability management, and network access control (NAC). We connected subject matter experts from each location to leverage their expertise in establishing or aligning these three technologies.
* For vendors used at both UC locations, we realized savings by negotiating pricing and terms for both locations simultaneously. In some cases, we saved time by discussing both UC locations during one regular check-in meetings with key vendors.
* We reduced some duplicative work by sharing vendor risk assessments between the two UC locations.
* We were able to advance biomedical device security by sharing information and connecting groups at both locations, and commissioning third-party biomedical device security assessments that will help both locations mature their programs.
* CISO salary and benefit costs were split between both locations.

Initially, the arrangement was intended to last for one year, but due to the success of the pilot, the arrangement continued for much longer. Ultimately, the locations chose to end the arrangement due to ever-increasing CISO responsibilities at both locations, but the program delivered clear value to the University of California. The experiment helped further the UC Health goal of improving the lives of all people living in California by improving protection of our data, systems, and reputation.