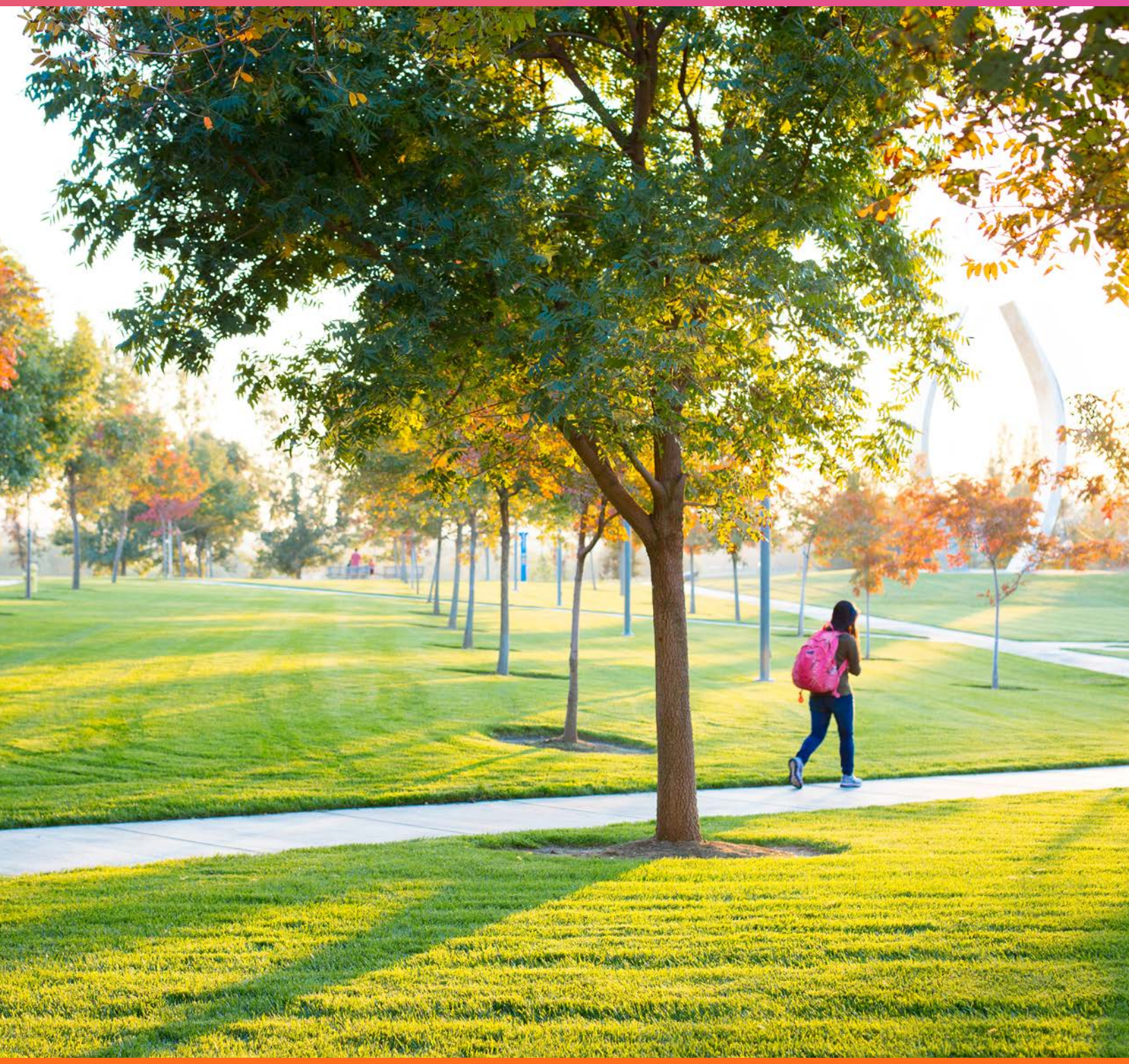
UC Cyber Risk Program

2023 REPORT

UNIVERSITY OF CALIFORNIA



UC is leading the way in higher education by looking beyond cybersecurity risk management to embrace and uniquely define a vision centered on digital risk management. While the breadth of activities is extensive, digital risk management remains rooted in the shared building blocks of effective cybersecurity risk management, encompassing people, processes, tools, and governance.

VAN WILLIAMS, Vice President of IT and Chief Information Officer, University of California

Welcome

In the Cyber-Risk Coordination Center, our team approach to cybersecurity includes five pillars: governance, management, technology, environment, and culture. Together, we strive to establish strong partnerships, strategically align with UC locations, and foster a learning environment. Our team, collectively comprising more than 50 years of cybersecurity experience, includes Cecelia Finney, Farrokh Khodadadi, Adrian Mohuczy-Dominiak, Jackie Porter, and Wendy Rager. Read more about this talented team throughout the report and see a list of their professional certifications on page 25.

This year's annual report shines a light on the people throughout the University of California and the initiatives they're spearheading to make UC, and all of us, more cyber safe. For example, UC has been growing its pipeline of human resources, nurturing a diverse and informed workforce, conducting risk assessments across the university, and promoting cyber safe training and events.

We also introduced the concept of digital risk in 2023, which we define as risk posed by areas such as cyber security, digital accessibility, data privacy, IT third-party risk management, and emerging technology—these are interlocking pieces of a larger digital risk landscape. We began introducing the concept during the new UC Tech Academy: Cyber Leadership Program for UC leaders (read more about this program on page 6). Look for future opportunities to learn more about digital risk in the coming year.

Thank you for contributing to our success as a university!

MONTE RATZLAFF
Director, Cyber Risk Program
Interim Systemwide Chief Information Security Officer
University of California, Office of the President

TABLE OF CONTENTS

Cyber Risk Management at UC

Our approach to cybersecurity is structured around five pillars.

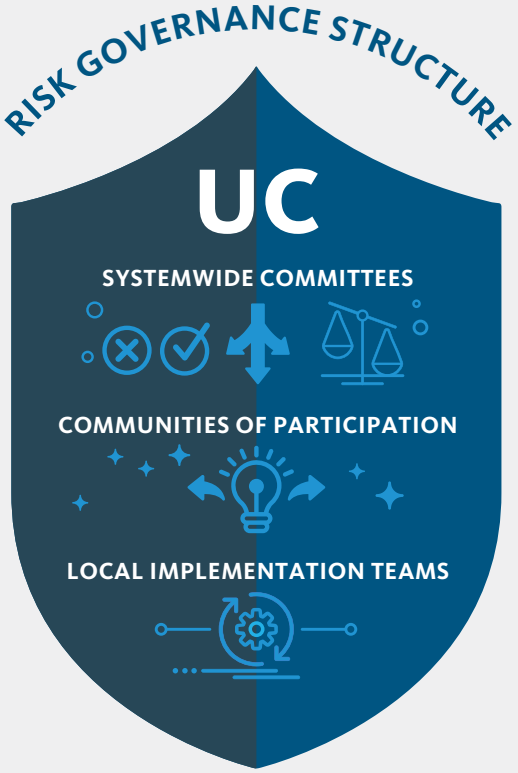
GOVERNANCE
Enhancing governance structures helps us coordinate cybersecurity efforts.

MANAGEMENT
Strengthening risk management ensures consistent efforts across the UC.

TECHNOLOGY
Adopting modern technology keeps UC one step ahead of threats.

ENVIRONMENT
Fortifying our environment through information sharing guarantees dependable protection.

CULTURE
Driving culture change makes sure every stakeholder plays their part.



Cybersecurity improves when everyone works together

Our risk governance structure contains three types of groups. These groups balance knowledge of systemwide requirements with proactive customized plans of protection for each campus, health center, and lab.

SYSTEMWIDE COMMITTEES:

- → Cyber Risk Governance Committee
- → IT Leadership Council
- → UC Information Security Council
- → Ethics, Compliance, and Audit Services
- → University Committee on Academic Computing and Communications

COMMUNITIES OF PARTICIPATION:

- → UC Security Incident Response Coordination
- → IT Policy and Security

LOCAL IMPLEMENTATION TEAMS:

- → Leveraging Scale for Value
- → Center for Data Driven Insights and Innovations

CAMPUSES HEALTH CENTERS LABORATORIES

UC at a Glance

10
CAMPUSES

6
ACADEMIC HEALTH CENTERS

3
NATIONAL LABORATORIES

850
DEGREE PROGRAMS

160
ACADEMIC DISCIPLINES

294,662
STUDENTS

328,900
EMPLOYEES

529,000
JOBS SUPPORTED

Tools and Services Catalog

Premier tools and services are provided to UC campuses, health centers, and labs to ensure that they are equipped with the best cybersecurity management to protect institutional information and IT resources. Learn more about these special tools and services that make UC a safer place to work, learn, and conduct research.

THREAT DETECTION AND IDENTIFICATION (TDI)

The Threat Detection and Identification (TDI) program is a collection of cybersecurity tools, services, and expertise that helps UC identify cybersecurity potential threats, provide network and endpoint visibility, and enable a better understanding of threats and vulnerabilities. TDI harnesses UC and third parties to give UC a common view of security systemwide, which is critical to informing readiness, allocating budget, and measuring risk reduction while also consistently identifying bad actors, malware, and system compromises—enabling a rapid, uniform response.

Attack Surface Management (ASM)

ASM services continuously monitor, identify, and manage the cybersecurity vulnerabilities and potential attack vectors in the cloud and on-premise infrastructures from the attackers' point of view.

Digital Threat Monitoring (DTM)

DTM provides early warning of malicious targeting and potential attacks with visibility into the open, deep, and dark web. This crucial component of the TDI program provides the ability to anticipate threats, sophisticated attack campaigns, breaches, and data leaks.

Leaked Credentials

If a compromised UC user credential is found, the relevant UC location is notified so action can be taken to determine if the password was reused and help the user reset their password.

Suspicious Domain Alerts

Suspicious domains are reviewed, and when a potentially malicious domain is found, the relevant UC location is notified so action can be taken.

Managed Detection and Response (MDR)

Around-the-clock monitoring and alert prioritization working with a range of third-party network, server, and endpoint technologies—on-premise and in the cloud. This service consumes alerts, investigates and analyzes attacker behavior, and performs advanced detection and threat hunting, pairing it with rapid response and remediation to amplify each UC locations' security operations team.

Protection of Network and Endpoints

A common standard is established to leverage expertise across the UC system and to share, track, and respond to cyber incidents in a coordinated fashion. These tools that protect hardware, software, networks, servers, and endpoints are available to all UC locations.

Security Operations Platform

This smart and adaptive platform enables analysts to have visibility across environments, detecting threats with machine learning, AI, and integrated real-time cyber intelligence. It predicts and prevents emerging threats, identifies root causes, and responds in real time.

INCIDENT RESPONSE COORDINATION

Incident response coordination services provide an organized and systematic approach to a cybersecurity incident or breach and communicate information about the situation.

Breach Notification

This third-party streamlined notification service provides protection from all angles with data breach readiness and response strategy using the latest market insights and trends. Extensive customer notification services include call center reports, mail notification services, and identity protection services.

Incident Response Coordination and Communication

During a cyber incident, a systemwide coordination and communication process is initiated to ensure that all executive stakeholders are informed as details become known. This process also involves internal experts in legal, privacy, compliance, and communications.

Systemwide Incident Escalation Report and Notification (SIREN) Tool

During an information security incident, potentially significant incidents are recorded, updated, and managed in SIREN for shared visibility.

THREAT INTELLIGENCE

Threat intelligence services include obtaining cyber threat information from a variety of sources to protect UC.

Cyber Threat Intelligence Services

The cyber threat intelligence service uses a third party with decades of security expertise to synthesize UC's raw data and deliver improved visibility into tactics that attackers employ, actionable insights, and context around threats.

Threat Intelligence Collection and Sharing

Partnering with a wide variety of local, state, and federal organizations as well as other third-party experts, UC shares threat intelligence and gains valuable insight and visibility into threats occurring right now. Subscriptions include intelligence on cyber threats, cybercrimes, trends from global operation centers, vulnerability analysis, dark web monitoring, industry local threats, and more.

SECURITY RISK ASSESSMENTS

Security Risk Assessments performed at UC locations, supplier, and health affiliates help the University of California manage cybersecurity risks.

UC Location Risk Assessments

Campuses, health centers, and labs across UC work together to identify, evaluate, and prioritize potential threats, vulnerabilities, and risks to information assets.

Supplier Risk Assessments

The cyber risk assessment unit works with UC locations on supplier risk to analyze threats introduced to UC via relationships from suppliers, partners, affiliates, contractors, or service providers. Assessments follow an established systemwide methodology with standard metric tracking.

Security Risk Assessments at Health Affiliates

Security Risk Assessments at existing and new health affiliates are coordinated on a regular basis to identify, evaluate, and control potential vulnerabilities to information assets at UC health centers.

CONSULTING SERVICES

Consulting services are available to assist UC locations in assessing their readiness levels. Services are paired with existing technologies, services, and operations with mitigation practices to manage the financial impacts of data breaches.

Digital Forensics

Digital forensics (also known as computer and network forensics) services involve coordination with forensics experts to perform investigations during and after an incident. These investigations help determine what happened, how and why it happened, and whether/what data was extracted.

Tabletop Exercises

Tabletop exercises are learning activities led by a third-party facilitator to simulate a real cyber event. These exercises evaluate cyber crisis responses and are invaluable to ensure stakeholders understand their roles, test communication and knowledge, uncover process gaps, and showcase how much is already known from the past.

Penetration Tests

Penetration tests leverage deep knowledge of threats and attack behavior using the tools, tactics, and procedures seen daily during incident response engagements. UC locations use penetration testing to identify vulnerable assets and receive strategic recommendations for security improvements.

TRAINING AND AWARENESS

Mandatory and customized cyber security training includes a mix of coaching, courses, and certifications to raise awareness and bridge skill gaps. Events, programs, communities, and tools provide additional opportunities for education and knowledge sharing.

Mandatory Cybersecurity Training

Faculty and staff participate in an annual mandatory training that provides up-to-date security awareness education that meets UC standards.

Customized Training Modules

In addition to mandatory training, optional modules are available on a range of topics including cyberattacks, remote work habits, social media, phishing, ransomware, data protection, deepfakes, AI, password security, privacy rules and regulations, and much more. Over 1400 knowledge articles provide an opportunity for self-learning.

New! Applied Intelligence Mentorship Program

The eight-month UC Tech Academy: Applied Intelligence Mentorship program consists of monthly modules or workshops that help attendees build and improve their UC locations' Cyber Threat Intelligence (CTI) programs, advance workflows, align CTI initiatives with business needs, and enhance systemwide communication.

Information Technology Policy and Security Community (ITPS)

The ITPS group is focused on sharing information related to the cybersecurity community, such as best practices, case studies, regulatory changes, initiatives, training, and more.

Systemwide Cyber Champions

Cyber Champions is a systemwide workgroup whose goal is to strengthen UC's culture of cybersecurity by empowering employees to help ensure safe computing. Champion team members partner with campus locations and health centers to create systemwide resources and provide support as cybersecurity enhancements are made.

UC Cyber Risk Program Annual Report

The UC Cyber Risk Program Annual Report features stories from all over the UC system, spotlighting the cybersecurity programs, initiatives, tools and services available to the UC system, and people making UC cyber safe.

UC Cyber Security Summit

The UC Cyber Security Summit is a forum for stakeholders and thought leaders to gather and share perspectives, discuss the latest in cybersecurity, network and meet new professionals, and learn practical day-to-day security tips to stay ahead of the curve.

Phishing Simulation Tools

UC leverages some of the world's leading phishing simulation tools to educate users, find vulnerabilities, and protect the UC system from threats as they emerge.

POLICIES, STANDARDS, AND GUIDELINES

Protecting institutional information and IT resources is a collective responsibility shared across the UC system. C3 leads changes to policies, standards, and guidelines through a collaborative community and communicates updates systemwide. Changes in regulations are reviewed, and updates to content are made as necessary.

Investing in Future Cybersecurity Leaders

Developing and investing in cybersecurity professionals and students is a must to keep up with the ever-evolving threat landscape. To support current and future leaders, new Cyber Leadership and Applied Intelligence Mentorship programs were developed to provide additional education, collaboration, and connection to cybersecurity professionals. The Women in Cybersecurity partnership and the summer intern program offered opportunities for participants to grow and learn, helping develop future cybersecurity leaders.

Cyber Leadership Program

In June 2023, UC launched the inaugural UC Tech Academy: Cyber Leadership Program for UC leaders designed to cultivate broad, diverse, and collaborative ways of thinking about managing digital risk. This unique program embodies the idea that cybersecurity progress means enhanced human harmonization, underscoring that it's not solely a technological responsibility. The program aims to equip participants with a common language, a unified understanding of UC's complex governance and management ecosystem, and a shared set of tools and skill sets for effective leadership.

The program brought together forty UC leaders from diverse areas such as information security, privacy, legal, risk, audit, compliance, law enforcement, and public safety—areas that partner with cybersecurity to manage UC digital risk. Participants attended two three-day modules at the UC Berkeley campus to learn about current and emerging cybersecurity issues, negotiation, conflict resolution, communications, and strategic thinking. UC Berkeley's Haas School of Business, UC executives, and industry and public sector experts taught the courses.

> *"The program has exceeded my expectations. In time, we'll achieve UC's goal to develop an effective, broad-based, and adaptable approach to managing digital risk that both advances UC's mission and strengthens our position as the world's leading social-impact university.*
>
> **VAN WILLIAMS, Vice President of IT and Chief Information Officer, University of California**

> *"The participation pool was pretty diverse, which exposes everyone to a large set of diverse perspectives. We had highly talented and intelligent folks from legal, audit, compliance, public safety, and information security attend.*
>
> **HENRY JENKINS, Senior Director, UC Irvine**

Internship Program

To contribute to the future cybersecurity workforce, the Office of the President employed interns from different UC campuses in the summer. The interns worked in various disciplines and applied their skill sets to real-world projects and problems. During their time, the interns participated in multiple activities and brought fresh perspectives and innovative ideas to the team.

Jade Gregory, a senior at UCLA majoring in Data Science and Statistics, interned with the Cyber-risk Coordination Center (C3) and applied her knowledge of numbers to many projects within the group. In her second week alone, Gregory's impact was felt after she solved a data mystery with the first Gramm-Leach-Bliley Act compliance report. "Figuring out the problem gave me the confidence I needed to be successful in this position," Gregory said.

In her role, she attended the UC Tech conference, contributed to the systemwide cybersecurity metrics, applied data interpretation and visualization techniques for the threat detection and identification program (TDI) program reports, and summarized data for the Board of Regents.

> *"From the projects I worked on, I've become more aware of how prevalent cybersecurity truly is in our everyday lives. I have even more interest in pursuing cybersecurity now that I've garnered a deeper understanding of the fast-paced environment that protects and benefits the population daily.*
>
> **JADE GREGORY, 2023 Intern, Rising Senior at UCLA**

Women in CyberSecurity

Women are a minority in the cybersecurity field, both as an area of study and a profession. One of UC's core values is diversity, equity, and inclusion, so partnering with an organization that supports women in cybersecurity in our student body and workforce is a natural fit. The Office of the President initiated this partnership with Women in CyberSecurity (WiCyS), an organization of nearly 8,100 members dedicated to uniting women from academia, research, and industry to share knowledge, network, and mentor others. The global nonprofit, which was started in 2013, is an important resource in helping women develop their skills and advance their careers.

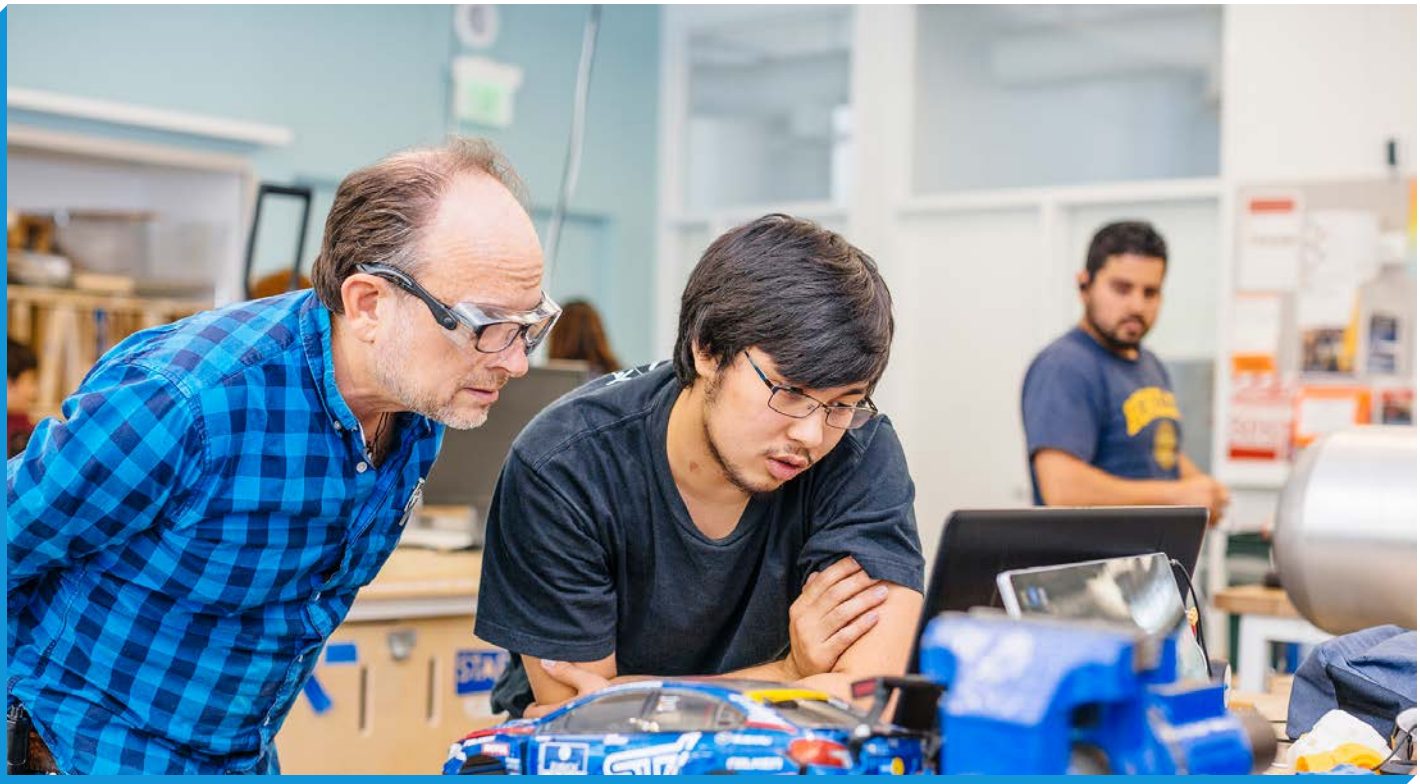
This strategic partnership will help ensure that UC continues to provide opportunities to help women advance in cybersecurity throughout every stage of their careers, building a stronger, gender-diverse cybersecurity workforce and a more robust educational entity.

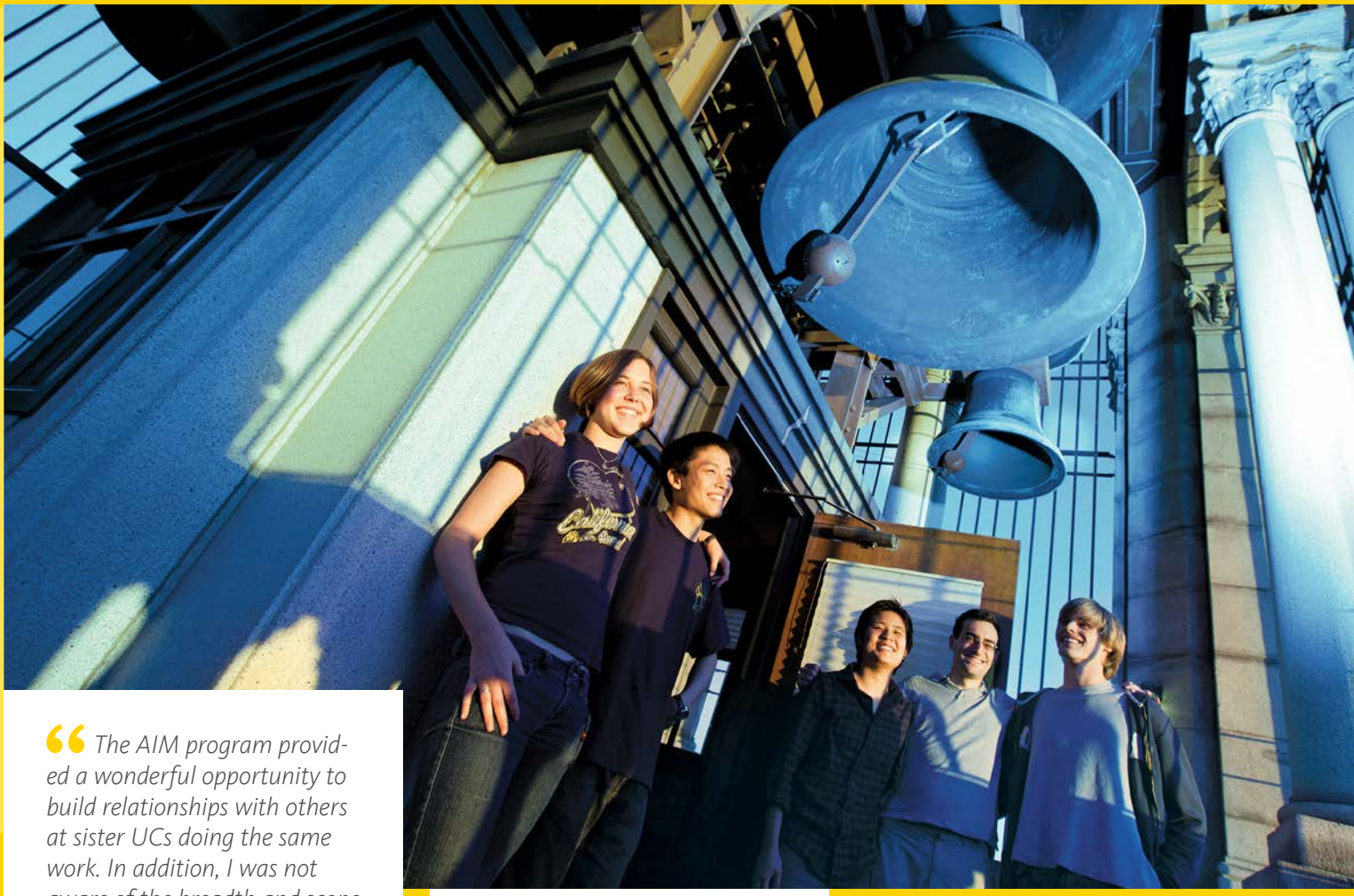
Applied Intelligence Mentorship Program Helps Build Cyber Threat Intelligence Across UC

Twelve Cyber Threat Intelligence (CTI) practitioners across UC had an opportunity to enroll in the first cohort of the UC Tech Academy: Applied Intelligence Mentorship (AIM), an exciting new CTI program developed in partnership with the UC Cyber-risk Coordination Center and a third-party partner. The eight-month virtual program consisted of monthly hands-on workshops and modules where participants learned about building and refining UC locations' CTI programs, optimizing workflows, aligning CTI initiatives with business needs, and improving systemwide communication. In addition, attendees gained insight into how to immediately implement what they learned, met peers across UC with similar settings, and developed a professional network. Since taking on threat intelligence isn't always intuitive, the program helped teach people how to better incorporate CTI into their work.

The program's goal is to have as many people as possible across UC understand how to leverage cybersecurity to reduce risk by staying ahead of the curve. The first cohort was a success, and the second cohort began in December 2023.

> *"The program added concrete principles and approaches to CTI, which were presented in a much more holistic fashion that the many resources I've read and cataloged while learning about CTI over the years. While CTI resource allocation, scale, and maturity will vary greatly from organization to organization, having the underlying principles and approaches to inform the level of investment and focus is key to communicating capability and residual risk to leadership.*
>
> **TOBY BARBER, Information Security Architect, UC San Francisco**





"The AIM program provided a wonderful opportunity to build relationships with others at sister UCs doing the same work. In addition, I was not aware of the breadth and scope of CTI. Going through with the process the team outlined has helped highlight the opportunities for improvement in how I categorize CTI-related work as well as help contribute towards those efforts at our campus.

DON KILEEN, IT Security Analyst, UC Santa Barbara

"The course topics were pretty broad and covered everything from setting up a CTI program to what to look for and how to go about it. So whatever step your organization may be in the process, there is useful information.

MIGUEL SALAZAR, Computer System Engineer, Lawrence Berkeley National Laboratory

14th Cyber Security Summit: Old, New and Learn What to Do

The excitement was palpable at the 14th Cyber Security Summit, the first in-person summit since 2019. Participants became reacquainted at the gathering, held at UCLA Carnesale Commons. More than 200 people from functional areas such as IT security, legal, procurement, compliance, and more came together to share ideas, learn from each other, and network with colleagues. The evening's gathering was a favorite, as attendees had time to continue conversations and meet new professionals. Speakers included industry experts and sponsors who spoke about a variety of topics related to cybersecurity.

Presentations Included:

US Government Cyber Case Studies: Lessons Learned
Olivia Olson, Assistant Special Agent in Charge, Cyber & Counterintelligence Branch, FBI Los Angeles

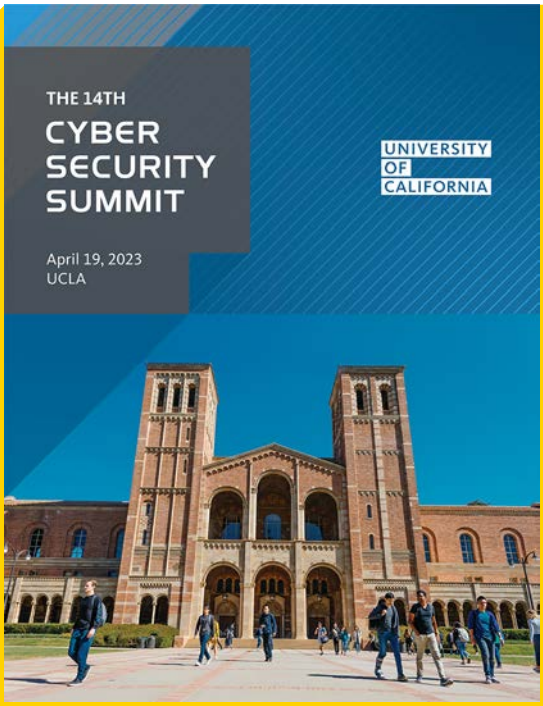
Cameron Schroeder, Chief, Cyber & Intellectual Property Crimes of United States Attorneys' Offices, DOJ Los Angeles

How to Develop a Security-First Mindset
Jenny Brinkley, Director of Amazon Security

Privacy Enhancing Technologies: From Theory to Practice
Dr. Rafail Ostrovsky, Norman E. Friedmann Distinguished Professor of Computer Science and Mathematics, UCLA

Law and the CISO
Sajjad Matin, Principal Counsel for Cybersecurity and Data Protection in the UC Office of General Counsel

Franklin Monsour, Jr, Partner at Orrick, Herrington & Sutcliffe LL



ATTENDEE DATA

46% FIRST TIME

19% 4+ SUMMITS

SATISFACTION RESULTS

97% Of participants were very satisfied or satisfied with the overall event

100% Of participants were extremely likely or likely to attend and recommend our summits to a colleague

> *Loved the discussion with US government case studies... I gained the most valuable information by talking to other conference attendees—learning about their experiences and what they're currently working on.*
>
> SUMMIT ATTENDEEE

> *The feds and lawyer talks covered some material new to me, and the case studies presented alarmed me sufficiently to do some planning.*
>
> SUMMIT ATTENDEEE

Cybersecurity Awareness Month

This October marked the 20th year of Cybersecurity Awareness Month, a dedicated month established by the President of the United States and Congress for government and industry together to raise cybersecurity awareness.

This year's theme focused on protecting your digital self and your data. With increasing digital threats and evolving technologies, being aware of online risks is more important than ever. UC focused on key behaviors that people can use to protect themselves in their personal lives and at work.

UC offered more than 15 systemwide events and numerous individual UC location events to support the campaign. Events included live webinars, lectures, panel discussions, social engagement, and games. Topics included health device security, cyber leadership, cybercrime, AI, and social engineering.

CYBERSECURITY AWARENESS MONTH | OCT 2023

Cybersecurity Month Highlight

JEOPARTY GAME!

Lia Grant, Assessments Security Analyst with the UC Berkeley Information Security Office, crafted a cybersecurity game called JeoparTy, based on the Jeopardy game. JeoparTy tested users' cybersecurity knowledge of definitions, acronyms, passwords, and the internet. To add to the fun, a "Stump the CISO" version of the game tested our CISOs' cybersecurity knowledge!

> *I thought this was a fun event, and I can see how it could be used to reinforce cybersecurity concepts and create engagement. Great job!*
>
> **JULIE GOLDSTEIN, Information Security Policy Program Manager, UC Berkeley**

For more information about being safe online, see our story about privacy courses on page 22.

Phishing Campaigns at UCLA Health

Phishing and stolen or compromised credentials were responsible for 16% and 15% of breaches, respectively, with phishing moving into the lead spot by a small margin over stolen credentials, which was the most common vector in the 2022 report.*

Phishing remains a major cybersecurity concern within UC, as cyberattacks become progressively more sophisticated and frequent every year. To address it, UCLA Health began running complex phishing campaigns for all 50K+ people at UCLA Health with the goal of motivating people to report phishing attempts—not just ignore them.

Luis Perez, Senior Information Security Analyst at UCLA Health, stated, "We wanted to focus on the human layer, which is often the most exploited by cybercriminals, to build a strong security culture in the organization and equip all our users with the knowledge and confidence to respond and report in the event of a real-life attack."

The campaigns introduced more complex examples from global real-world attacks as well as other challenging scenarios, such as a simulated attack from a compromised UCLA Health email account.

Another unique aspect of the campaigns involved a targeted and tailored training approach. It allowed UCLA Health to educate, continuously remind users how to report, and reward those who reported with Cybersecurity Challenge points that increased their chances of winning raffle prizes.

The phishing campaign's year-over-year report rates increased despite more users and higher difficulty levels. The UCLA Health fail rate remains well below the health care and education industry.

*Source: IBM Cost of a Data Breach Report 2023, IBM Security

UCLA Health

124%

Increase in reporting phishing attempts after implementing campaigns

86%

Web application attacks involve stolen credentials

75%

Ransomware attacks originate with surface exposures

74%

Breaches that involved a human element

Sources: Verizon Data Breach Investigations Report 2023; Palo Alto Unit 42 Ransomware and Extortion Report

UC Berkeley's Lily L. Chang Capstone Award Honors Top Cybersecurity Projects

At UC Berkeley, students can prepare for the workforce and their future in many ways. One example is in the Master of Information and Cybersecurity (MICS) program, where students participate in capstone projects during their final semester to demonstrate the cybersecurity technical and professional skills acquired during the program. The capstone projects showcase core cybersecurity technical skills, understanding how cybersecurity issues impact humans, and professional skills—proficiencies that prepare students for success in the field.

The top projects receive the Lily L. Chang MICS Capstone Award, established in 2019 through a gift by Lily L. Chang. Chang is a career technologist and business leader dedicated to cultivating security professionals. She first established the Dr. James R. Chen Award in 2001 in memory of her late husband, a scholar at NASA, for the winning final project of the Master of Information Management and Systems (MIMS) program. Chang was inspired to create the capstone award when she attended UC Berkeley's commencement and heard about the new MICS program. Previously the VP of the Strategic Transformation Office at VMware, Chang is currently on the Women Who Code Board and is an adjunct lecturer for Santa Clara University Leavey School of Business.

Receiving the Lily L. Chang Award marks the beginning of a successful journey into the cybersecurity field for MICS students.

Berkeley
UNIVERSITY OF CALIFORNIA

UC San Francisco Deploys Attack Surface Management

Attack Surface Management (ASM) is the continuous remediation and monitoring of cybersecurity vulnerabilities and potential attack vectors. UC San Francisco became an early adopter of ASM services when they added the capabilities to their cybersecurity monitoring program. The ASM tools continuously scanned UC assets from the perspective of an internet attacker to find vulnerabilities.

The ASM service allowed UC San Francisco to rapidly improve exposure management for their public-facing digital assets, and it also propelled the automatic discovery and assessment of their constantly evolving digital asset inventory on their network and in the cloud. These services enabled the team to quickly prioritize risk and establish mitigation strategies for their diverse technology footprint.

UCSF
University of California
San Francisco

> *"These tools, combined with our processes, enable our goal as cybersecurity professionals to safeguard our colleagues in their use of technologies in UC San Francisco's clinical, research, business, and education missions.*
>
> **TOBY BARBER, Information Security Architect, UC San Francisco**

24.6% Faster

Organizations with an ASM solution identify and contain a data breach than those without one

Source: IBM Cost of a Data Breach Report 2023, IBM Security

Security Risk Assessments

The average cost of a data breach in 2023 was $4.45M.*

Bad actors focusing on software breaches with suppliers are on the rise, and they have the capability to inflict widespread harm that impacts both the main target and their customers. The Office of the President addressed the increased risk of data breaches by creating a new centralized unit to assess location and third-party supplier risk. The purpose of the new cyber risk assessment unit is to establish a repeatable risk methodology, reduce redundancies in current processes, and improve executive visibility. An added benefit is sharing risk assessment information across the system to make more informed investment decisions.

*Source: IBM Cost of a Data Breach Report 2023, IBM Security

UC Locations

The new cyber risk assessment unit will work with UC locations on self-cyber assessments to identify various risks that could affect UC assets, including hardware, systems, applications, laptops, research data, and intellectual property. UC location assessments will be performed in accordance with an established systemwide risk methodology and standard metric tracking.

Suppliers

Supplier assessments analyze the risks introduced to UC via relationships along its ecosystem or supply chain, which may include suppliers, partners, affiliates, contractors, or service providers with access to UC internal data, systems, processes, or other privileged information.

Health Affiliates

Security risk assessments at existing and new UC health affiliates are coordinated regularly to find potential cybersecurity vulnerabilities. Assessments help to ensure HIPAA compliance and keep patient records safe.

50+ Security risk assessments (SRAs) performed at University of California Health Community Affiliates

The University of California Health System teams up with UC Health Community Affiliates to provide medical care for patients. The partnership enables the affiliates to access UC's advanced healthcare records system. C3 manages the SRAs for the affiliates, helping to ensure HIPAA compliance and keep patient records secure.

Security Risk Assessments Minimize Risk at Health Affiliates

Part of the mission of the University of California Health (UCH) is to "deliver exceptional care that improves the health and well-being of all people living in California, the nation and the world." To help extend its reach, UCH partnered with Community Affiliates to exchange best practices and share the latest advancements in treatment and technology. The Community Affiliate clinics performed 865,000 ambulatory patient visits in 2022, accounting for 29.5% of the total ambulatory visit volume.

A component of the important partnerships involves the affiliates getting access to UC's patient record software, enabling patients to have a single medical record and making it easier for medical professionals to help patients. Given the sensitive nature of medical records, patient data, and financial data, health care organizations are a prime target for cyberattacks. In fact, for the 13th year in a row, the health care industry reported the most expensive data breaches at an average cost of USD 10.93 million.*

To minimize risk in providing access to affiliate providers, C3 coordinates SRAs. These evaluations systematically pinpoint and address potential cyber threats to affiliates and their critical information assets. Conducted at regular intervals, SRAs play a pivotal role in fortifying patient privacy and ensuring robust security measures.

*Source: IBM Cost of a Data Breach Report 2023, IBM Security

Policy Corner

Active Policies

IS-3 Electronic Information Security
IS-3 establishes a framework that ensures all UC locations follow the same approach to reduce and manage cyber risk, protect information, and support the proper functioning of IT resources.

IS-5 Licensing and Operations, University Radio, Television, and Microwave Facilities of University
The purpose of IS-5 is to set the minimum requirements and procedures for the licensing and operations of radio, television, microwave stations, and other FCC-licensed systems.

IS-12 IT Recovery
IS-12 was created to guide and prepare for IT Recovery and business continuity in the event of an unavoidable or unforeseen disaster, whether natural or human-made.

Resource Updates

The IT Policy Glossary includes more than 90 defined terms relevant to using UC's IT and information security policies and standards. This year, the formatting of the glossary was updated to make it easier to use.

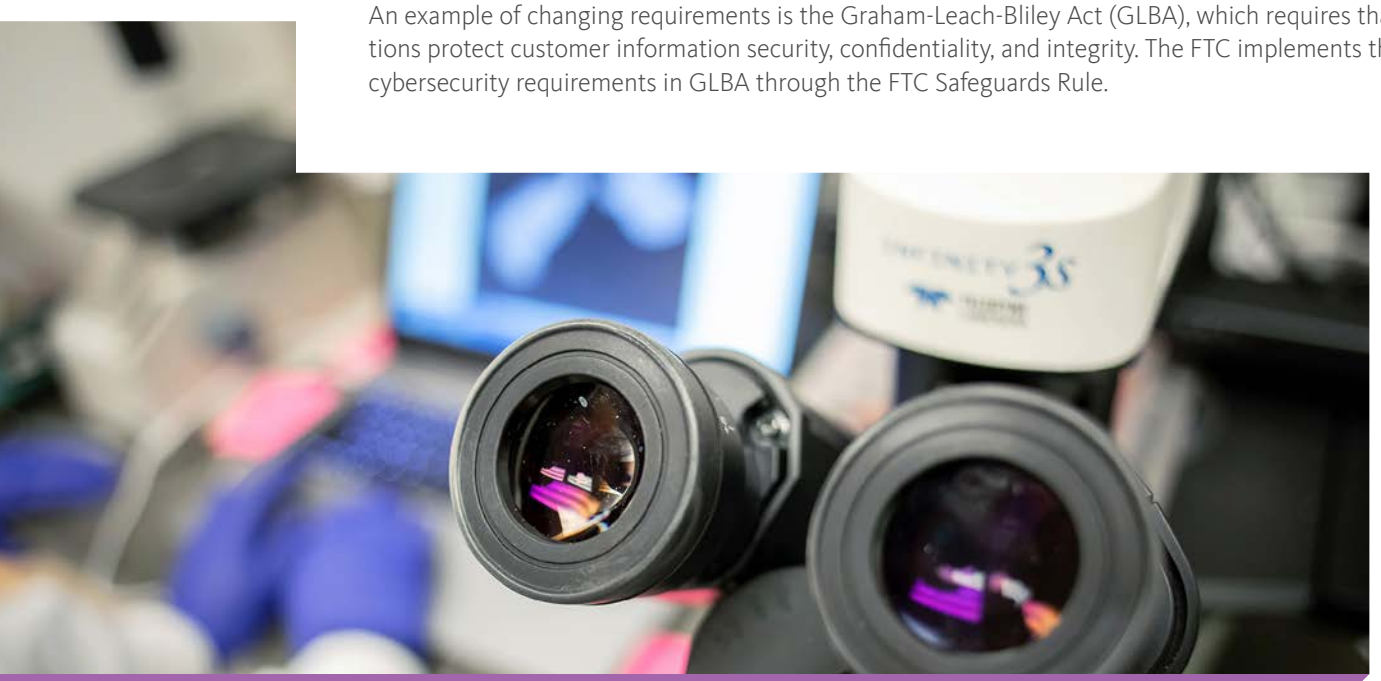
Sharing Best Practices

UC's IS-3 Electronic Information Security Policy establishes the framework for UC to achieve electronic information security goals. While IS-3 provides the structure, the individual UC locations make IS-3 actionable. To that end, UC Berkeley and UC San Diego each shared how they implemented IS-3 on their campuses during different Information Technology Policy and Security (ITPS) meetings this year. UC Berkeley shared their IS-3 implementation plan and focus, and UC San Diego focused on the roles and responsibilities associated with IS-3. Presentations like these enable the ITPS community to learn best practices from each other.

Staying Current with Rapidly Changing Requirements

No matter what changes occur in city, county, state, federal, global, and industry regulations, UC must stay informed, analyze changes, and ensure that our policies and guidance incorporate the latest requirements. The changes are recorded, requirements are mapped to policies and standards, collaboration with key stakeholders occurred, and the UC community is informed.

An example of changing requirements is the Graham-Leach-Bliley Act (GLBA), which requires that institutions protect customer information security, confidentiality, and integrity. The FTC implements the cybersecurity requirements in GLBA through the FTC Safeguards Rule.



ITPS Enables UC Security Professionals to Connect

Established in 2015, the Information Technology Policy and Security Community (ITPS) group has grown through word of mouth to include members who want to focus on major challenges, legal and policy issues, and campus security issues through collaboration and information sharing. This active community of participation meets monthly, 10 times a year, and has an average attendance of 150+ members. The community also communicates regularly outside of the meetings to share information about threats and vulnerabilities, best practices, trends, and other topics related to information resources. ITPS is open to anyone at UC with a role or interest in IT policy or cybersecurity.

Presentations Included:

Research Security Updates
Marci Copland, Systemwide Associate Director, Research Security and Export Control, Office of the President

Case Study
UC San Diego IS-3 Program and Status

IS-3 Implementation at UC Berkeley
Allison Henry, Chief Information Security Officer; *Scott Seaborn*, Campus Privacy Officer; *Julie Goldstein*, Info Security Policy Program Manager

Case Study
An Identity Makeover: Transforming a Campus IAM (Identity and Access Management) System *Sureyya Tuncel* and *Dewight Kramer*, UC Riverside

One Year as CISO
April Sather, Chief Information Security Officer, Office of the President

Trends in Cybersecurity and Privacy Litigation
Jerome Mayer-Cantú, Principal Counsel, Litigation, UC Office of the General Counsel

Trackers, Cookies and Litigation
Hillary Noll Kalay, Principal Counsel, UC Legal

We Are Not Alone: Leveraging Cross-Industry Insights for Higher Education Cybersecurity Success
Brian Kelly, Compass IT, VCISO

Digital Accessibility and Security: Why Not Both?
Judy Thai, Director of Application Engineering, Office of the President; *Trevor Finneman*, Principal Counsel, Office of the President

Social Media Privacy, Security and Safety
Monte Ratzlaff, Cyber Risk Program Director, Office of the President

IT Recovery and Business Continuity Planning
Tara Brown, Business Continuity Planner and *Adam Quilty*, IT Services Continuity Lead from UCLA; *Amina Assefa*, Director of Emergency Management & Business Continuity, Office of the President

Cyber Security Exercises with ITPS
Lony HaleyNelson, San Francisco Dept. of Emergency Management, Emergency Services Coordinator, Integrated Preparedness Team

Ransomware Playbook
Alex Lichtenstein, Program Manager of the Office of Emergency Preparedness, UCLA Health

ITPS Members

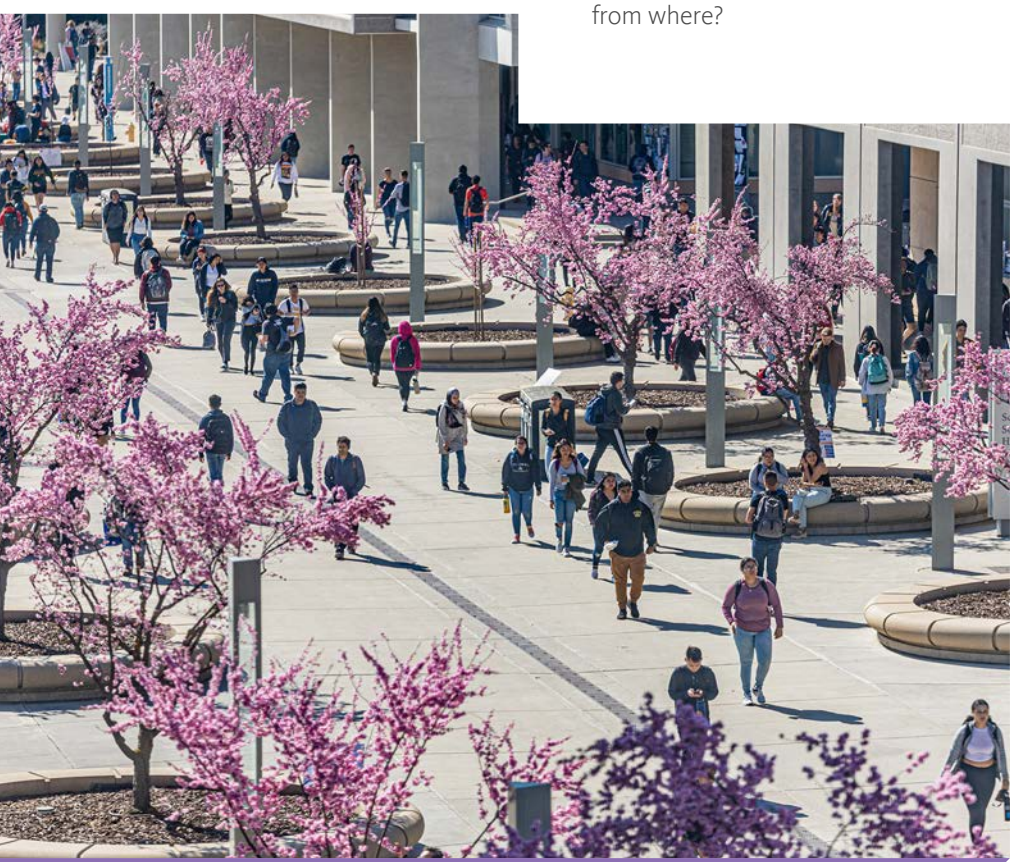
670 = 1,000% Increase in 8 Years

Collaborating for Cybersecurity: Unit Information Security Lead "As-a-Service"

IS-3 is the systemwide information security policy that ensures all UC locations follow the same approach to reducing and managing cyber risk, protecting information, and supporting the proper functioning of IT resources while leaving the implementation up to the UC locations.

A core requirement of IS-3 is for each unit to identify a Unit Information Security Lead (UISL). UISLs provide oversight and execution of information security responsibilities, including implementing security controls, reviewing risk assessments, reporting information security incidents to the CISO, and more.

Capacity has been the challenge for many units in fulfilling this role since its introduction in 2019. Effectively executing UISL responsibilities while continuing to deliver on existing priorities and projects is not easy. Additional resources would clearly be needed to meet policy requirements successfully. The question was—from where?



Chief Information Officer (CIO), Office of the President, Molly Greek, built a business case and secured organizational support for what is now known as Unit Information Security Leads "as-a-service." In early 2022, units started signing up for the service. The percentage of a UISL recommended for each unit was derived from the number of sensitive applications (i.e., classified as P3 or P4) in their portfolio. At the Office of the President, over 70% of units leverage the service, with the remainder naming existing staff to the UISL role. During the first year, the focus was ensuring a complete application inventory, reviewing access, measuring unit alignment to IS-3, and orienting units to the service. As UISL-as-a-service enters its second year, priorities will shift towards developing unit metrics and creating unit security plans and risk registers to share with leadership to bring greater visibility to cyber risk.

April Sather, Office of the President Chief Information Security Officer, shared that UISL as-a-service provides a dedicated cybersecurity capacity while building a community at the same time. "While our team provides the structure, technology, and guidance to help UISLs succeed, the relationships they build with one another, and with unit stakeholders, make the difference. This model slices through silos and builds bridges in a really effective way." The Office of the President's local security team also brings the UISLs together quarterly to share tools, techniques, and templates and hosts monthly lunch-and-learns on various topics.

Tabletop Exercises Focus on Coordination and Communication

When a cyber incident occurs, the response team must know their roles and responsibilities, and be prepared to act and communicate swiftly with the appropriate parties to mitigate cybersecurity impacts. The UC Information Security Incident Response Standard, stemming from the IS-3 Electronic Information Security policy, is the guiding systemwide cyber incident response coordination process.

In 2022, C3 held a workshop that tackled executive communication during a cyber incident and received rich feedback to improve the process. As a result, the process was updated, and training occurred within the Office of the President.

In the spirit of continuous improvement, C3 organized two tabletop exercises in 2023 to test the updated process. The goals of the tabletop were to raise awareness of expectations and identify gaps. Led by a third party, the two-part learning exercise simulated a realistic cyber scenario with twists and surprises—like a real cyber event—to test the team's response.

- **In part one,** the team followed the coordination and awareness process, including the communication methods. The group included C3, External Relations and Communications (ER&C), UC Legal, Privacy/Compliance, and subject matter experts.
- **In part two**, the team tested the communication process with select Office of the President executives, including the President's Executive Office.

In preparation for the exercises, the team gathered to review the process. The engaged team provided feedback and enhancements that will be a benefit in the future. The prep work and the exercises highlighted areas for further development and showcased how well the team was prepared for the exercise.

> *"Teams should always iterate on processes to discover gaps, make improvements, and test communication channels. As cybersecurity is constantly evolving, teams must be set up for success to be prepared for whatever may occur and minimize impacts to our people and communities.*
>
> **WENDY RAGER, Cyber-risk Coordination Center Manager, Office of the President**

Cost savings achieved
by organizations with high levels of incident response planning and testing

$1.49M

Source: IBM Cost of a Data Breach Report 2023, IBM Security

Live and On-Demand Privacy Courses

Privacy 101 Workshop: A Global, Live Training

Why does privacy matter? How does it relate to legal compliance, personal civil rights, and data practices? The Privacy 101 Workshop, a flagship privacy training that draws audiences worldwide, covers these topics and so much more. Since online privacy touches every aspect of life, this three-hour workshop is designed for anyone in any profession. Attendees learn about the four foundational types of privacy, the history and importance of privacy and data ethics, key privacy principles, privacy laws applicable to higher education, and practical steps to protect data at work and our own privacy.

Privacy @ UC San Diego Course: On-Demand

Based on the hugely popular Privacy 101 Workshop, the one-hour Privacy @ UC San Diego course was created in 2023 and is available on-demand via UC Learning. The training focuses on basic data privacy principles, relevant legislation, and UC policies applicable to campus activities. Those who work with personal data at P3 or above at UC San Diego are required to take the course. In the future, this course may be available to others outside of the university.

UC San Diego

> *"Privacy is about how we live our lives. It doesn't just touch criminals and famous people.*
>
> **PEGAH PARSI, Chief Privacy Officer, UC San Diego**

> *"Beyond FERPA - 45 minutes of an intense overview of the privacy compliance landscape, done masterfully.*
>
> **Privacy @ UC San Diego Training Participant**

Attendance

Privacy 101 Workshop

1,700

Attendees since 2020 inception

Privacy @ UC San Diego Course

300+

Attendees since its May launch

> *AI is used routinely now for things like malware analysis to identify malicious documents and malicious webpages. What we don't have are entities that are capable of reasoning. This is an opportunity to bring artificial intelligence and security together in a novel way.*
>
> **PROFESSOR GIOVANNI VIGNA, UC Santa Barbara**

$20M AI-Powered Cybersecurity Research Project Launched

UC Santa Barbara is leading a $20 million research institute for next-level AI-powered cybersecurity. The National Science Foundation-funded Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION) is an effort to bring continuous learning and reasoning of AI to security threats. Professor Giovanni Vigna, a computer science professor and cybersecurity expert at UC Santa Barbara, heads the multidisciplinary five-year project. Vigna is joined by UC Santa Barbara colleagues Chris Kruegel, João Hespanha, and Ambuj Singh, as well as more than 20 collaborators from UC Berkeley, Purdue University, Georgia Tech, The University of Chicago, University of Washington, University of Illinois Chicago, Rutgers, Norfolk State University, University of Illinois, and University of Virginia.

Singh, whose research involves AI/human interactions, said merging AI with human expertise is a best-of-both-worlds security scenario. "Building a joint human-AI system that complements each other with capabilities, such as presenting a human expert with risk-reward options derived from an AI-learned model, are some of the ways in which the institute will lead the frontier of future research in AI cybersecurity."

The research plan involves combining foundational AI with cybersecurity. An AI "stack" contains layers of functionality to support AI in various ways, including learning and reasoning with domain knowledge, human-agent interaction, multi-agent collaboration, and strategic gaming and tactical planning. These AI domains enable the creation of "agents" that will be able to assess and identify a potential attack, as well as identify the attacker and take action for recovery.

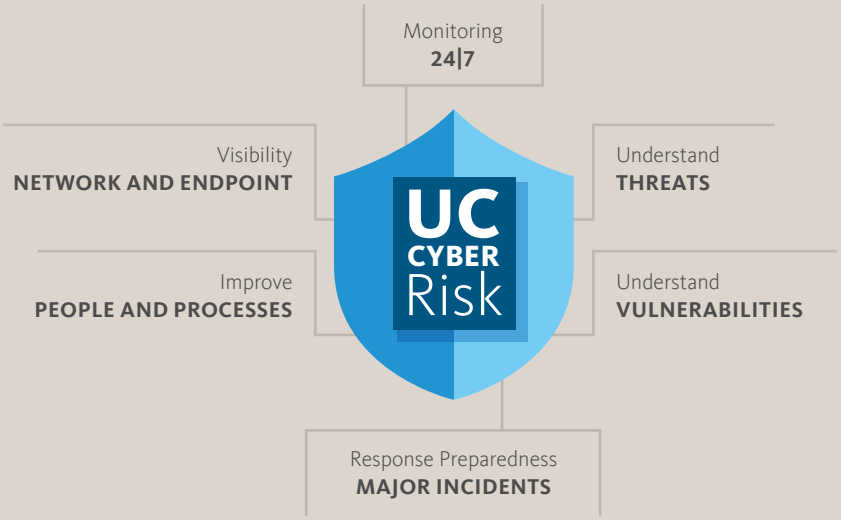
Per the National Science Foundation's website, the directors of the 25 AI Institutes presented their research on September 19, 2023, on Capital Hill "to enable congressional staff to learn more about the amazing research and technologies that are being developed at these AI Institutes."

Vigna said, "There is increased interest from lawmakers on AI-related issues in general and cybersecurity in particular. The advantages that stem from using autonomous intelligent agents to secure the nation's critical infrastructure are clear: AI-enabled terminologies will address the scale and time requirements for effective response to sophisticated attacks."

UC **SANTA BARBARA**

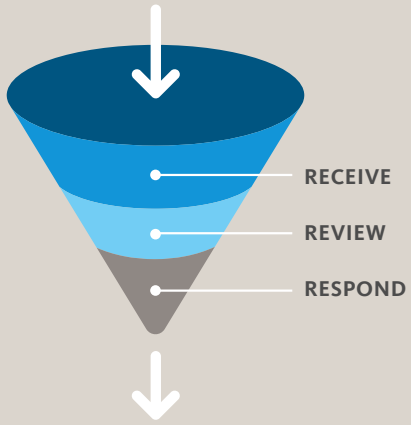
C3 at a Glance

Program Capabilities



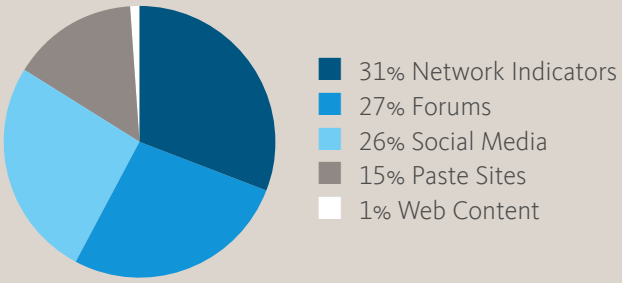
Alerts Analyzed

C3 identified threat vectors in these categories to reduce impact.

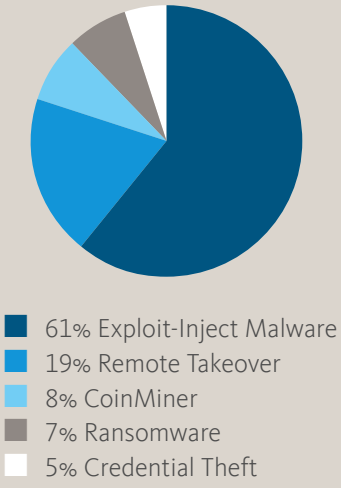


Digital Threat Monitoring

Digital Threat Monitoring enables us to analyze high-risk attacks from the open, deep, and dark web, as shown below, and then we can focus on the most significant threats.



Alert Types



TDI Investment

To support our TDI program, we invested in the following areas.

90% Monitoring and Response

8% Threat Visibility Expansion

2% Emerging and Detection Capabilities

84%

Of faculty and staff completed cybersecurity awareness training

C3 Team Members' Certifications

C3 team members hold multiple certifications in their fields.

- **Cisco**
  - **CCNA** Introduction to Networks
- **CWNP** Certified Wireless Network Professionals
  - **CWTS** Certified Wireless Technology Specialist
- **CompTIA** Computing Technology Industry Association
  - **A+**
  - **Linux+**
  - **Network+**
- **Cyber AB**
  - **CCP** Certified CMMC Professional
- **EC-Council** International Council of Electronic Commerce Consultants
  - **CEH** Certified Ethical Hacker
  - **CNDA** Certified Network Defense Architect
  - **ECSA** EC-Council Certified Security Analyst Certification
- **ISACA** Information Systems Audit and Control Association
  - **CISA** Certified Information Systems Auditor
  - **CISM** Certified Information Security Manager
- **(ISC)²** International Information System Security Certification Consortium
  - **CISSP** Certified Information Systems Security Professional
  - **ISSMP** Information Security System Management Professional
  - **CSSLP** Certified Secure Software Lifecycle Professional
- **ITIL** Information Technology Infrastructure Library
  - **4 Foundation**
  - **SOA** Service Offerings and Agreements
  - **OSA** Operational Support and Analysis
  - **PPO** Planning, Protection and Optimization
  - **RCV** Release, Control and Validation
  - **SO** Service Operation
  - **ITIL** Expert
- **Microsoft**
  - **MCP** Microsoft Certified Professional
- **PMI** Project Management Institute
  - **CAPM** Certified Associate in Project Management
- **SANS** SANS Institute
  - **GWEB** GIAC Web Application Defender
  - **GCCC** GIAC Critical Controls Certification
  - **GCFA** GIAC Certified Forensic Analyst
  - **GPCS** GIAC Public Cloud Security
- **Scrum Alliance**
  - **CSM** Certified Scrum Master
  - **SCPO** Certified Product Owner

The Landscape 2023

Cybersecurity threats often come down to the human element. IT teams are using security AI/automation and incident response testing to address cybersecurity concerns, and these technologies continued to have a positive impact on the 2023 landscape. At UC, we're bringing people together across campuses, health systems, and laboratories to collaborate and learn how to develop a systemwide security mindset.

Risks

- **$4.90M** average cost when phishing was the initial attack vector
- **$4.45M** average cost of a data breach
- **82%** of breaches involved data stored in the cloud—public, private, or multiple environments
- **74%** of breaches are driven by the human element
- **40%** of breaches are linked to hacking
- **24%** of attacks are linked to ransomware
- **16%** of breaches are linked to phishing

Benefits

- **108** days saved. Organizations with extensive use of security AI and automation identified and contained a data breach significantly faster than those with no usage
- **84** days saved. Attack Surface Management (ASM) helped accelerate total time to identify and contain a data breach by nearly 12 weeks
- **28** days saved. Organizations using threat intelligence were able to swiftly identify breaches, saving time and reducing vulnerabilities
- **51%** of organizations plan to increase security investments as a result of a breach. Top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies
- **39.3%** decrease in average cost of a data breach when an organization fully deployed AI and automation

Changes (2022 to 2023)

- **53.3%** increase in health care data breach costs (since 2020)
- **20%** decrease in cost with security AI
- **13%** increase in average cost of a ransomware breach
- **9.7%** increase in detection and escalation costs—remaining in the top spot as the costliest data breach expense
- **8.5%** decrease in lost business costs
- **2.5%** decrease in average cost of a data breach for organizations with 25,000+ employees
- **2.3%** average increased cost of each breach

Sources: IBM Cost of a Data Breach Report 2023, IBM Security; Verizon Data Breach Investigations Report 2023

Want to know more?

Contact Us
Monte Ratzlaff
Director, Cyber Risk Program
Interim Systemwide Chief Information Security Officer
University of California Office of the President

C3@ucop.edu