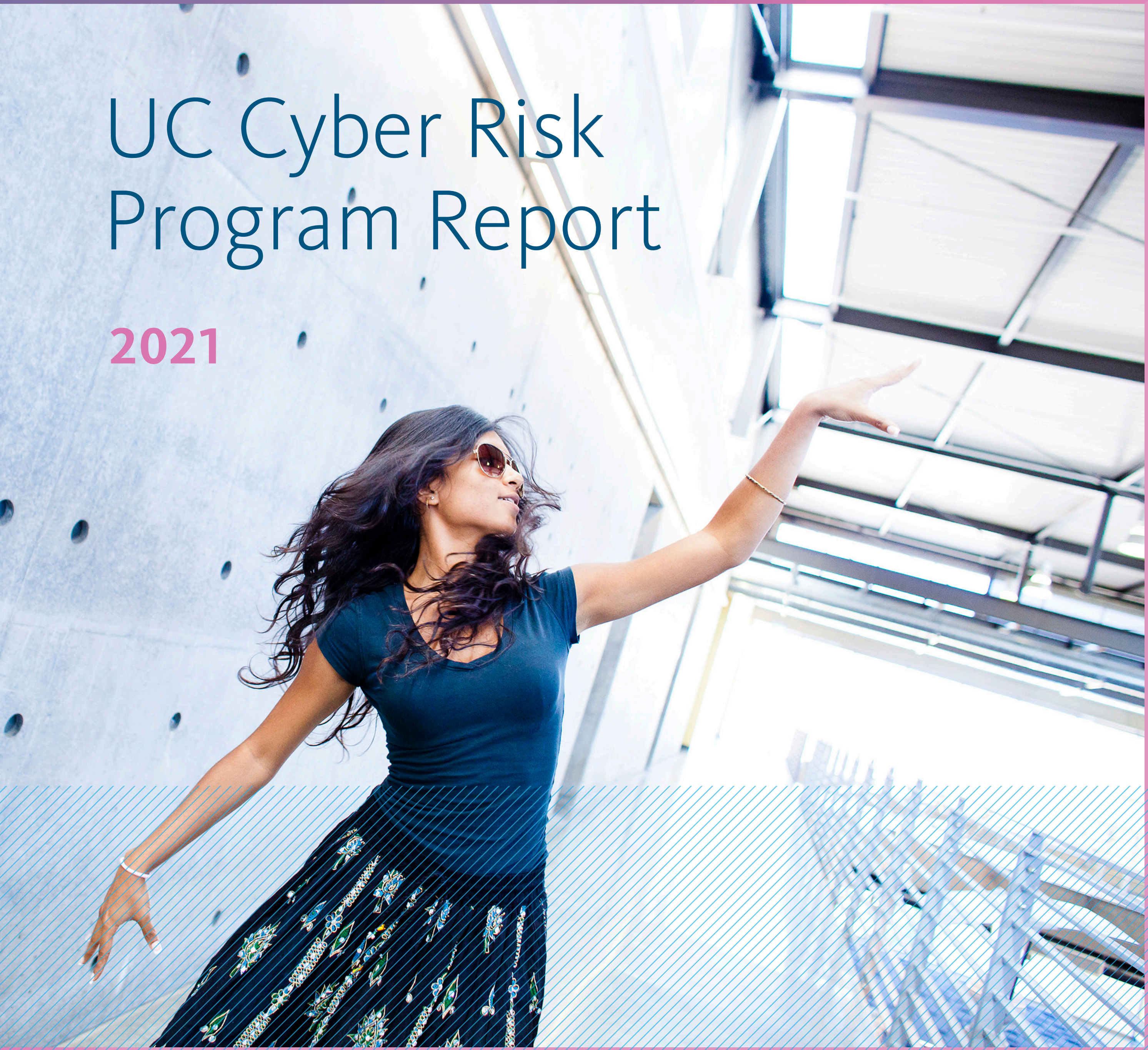


# UC Cyber Risk Program Report

2021

UNIVERSITY
OF
CALIFORNIA

# WELCOME

**Since its inception in 2015, the University of California's Cyber Risk Program has taken a coordinated approach to risk management.** We continue to emphasize the importance of building partnerships and creating opportunities for collaboration. Indeed, our most effective approach when facing challenges is to draw on the strength of our collective expertise.

We recognize the importance of vigilance and adopting a "security first" mindset for effective cyber risk management. Across UC we have worked together on best practices to decrease vulnerabilities, strengthen remote workforce systems and technologies, increase security awareness, and provide education, leadership, and support. This report provides details about the program's accomplishments in 2021 and our plans for meeting the challenges of the future.

The Cyber Risk Program relies on the contributions of hundreds of people across the UC system, from many different backgrounds. It is ultimately humans, not technologies, that are at the core of how we create effective cybersecurity. I look forward to cultivating a thriving community with you.

**Monte Ratzlaff**

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

# TABLE OF CONTENTS

“

*Technology is about the trust we build with our partners, customers, and colleagues, who look to us to amplify, accelerate and protect their work.”*

**VAN WILLIAMS**, VICE PRESIDENT FOR INFORMATION TECHNOLOGY SERVICES AND UC CHIEF INFORMATION OFFICER

# Meet Our Team Members

**The University of California Cyber Risk Program** includes the Cyber-risk Coordination Center (C3) and IT Policy Office. Our mission is to enable and facilitate the coordination of systemwide cyber risk initiatives that support UC's mission of teaching, research, and public service.

**MONTE RATZLAFF** Director, Cyber Risk Program,
UC Interim Chief Information Security Officer

**ROBERT SMITH** Systemwide IT Policy Director

**MATTHEW LINZER** Information Security Manager

**WENDY RAGER** Cyber Risk Coordination Center Manager

**ADRIAN MOHUCZY-DOMINIAK** Cyber Risk Technical Security Analyst

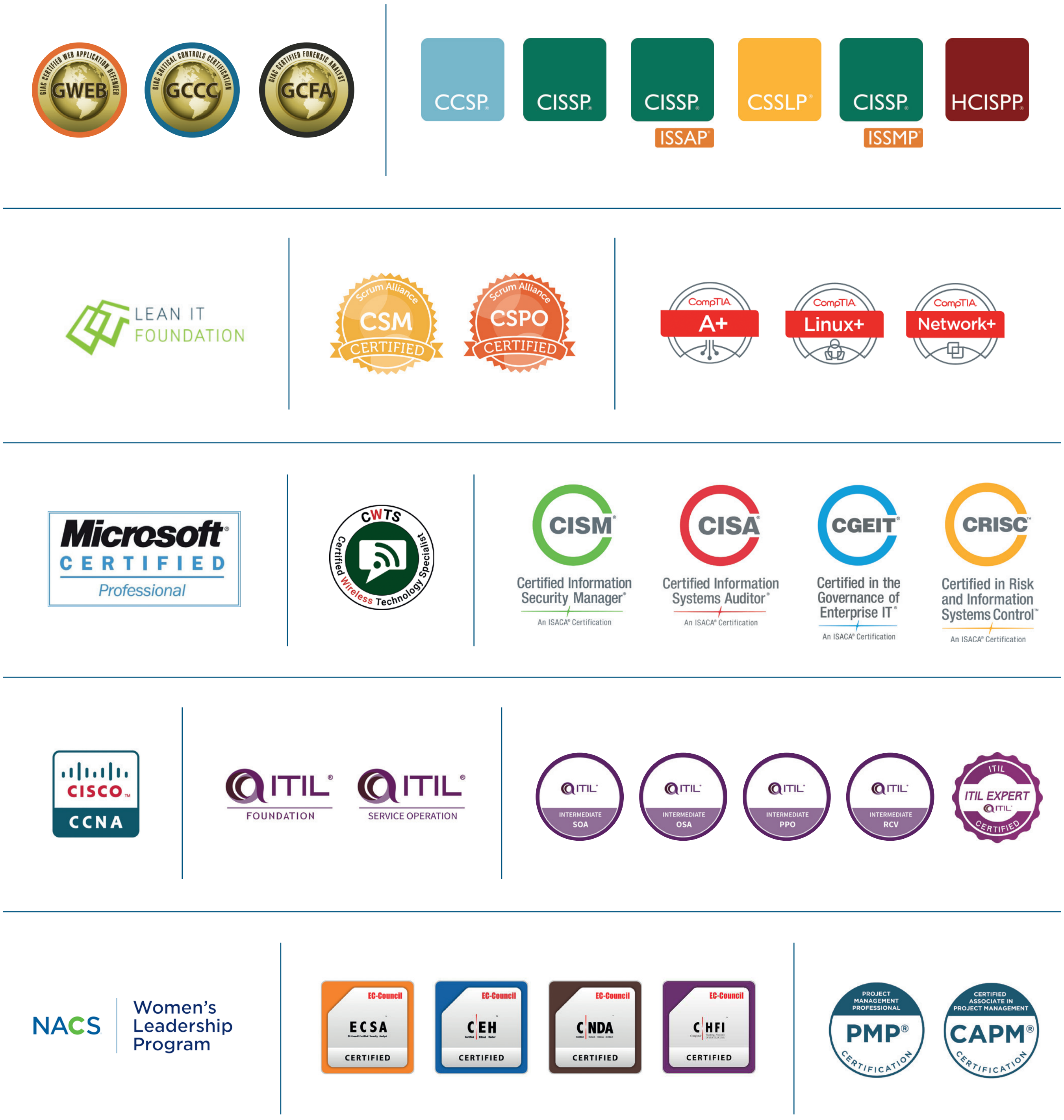
**CECELIA FINNEY** Cyber Risk Security Analyst

**FARROKH KHODADADI** Cyber Risk Technical Security Analyst

**JACKIE PORTER** Cyber Risk Project Coordinator

# Certifications

Our team members are experts who hold multiple certifications in their field.


GWEB
GCCC
GCFA
CCSP
CISSP
CISSP ISSAP
CSSLP
CISSP ISSMP
HCISPP
LEAN IT FOUNDATION
Scrum Alliance CSM CERTIFIED
Scrum Alliance CSPO CERTIFIED
CompTIA A+
CompTIA Linux+
CompTIA Network+
Microsoft CERTIFIED Professional
CWTS Certified Wireless Technology Specialist
CISM Certified Information Security Manager An ISACA Certification
CISA Certified Information Systems Auditor An ISACA Certification
CGEIT Certified in the Governance of Enterprise IT An ISACA Certification
CRISC Certified in Risk and Information Systems Control An ISACA Certification
CISCO CCNA
ITIL FOUNDATION
ITIL SERVICE OPERATION
ITIL INTERMEDIATE SOA
ITIL INTERMEDIATE OSA
ITIL INTERMEDIATE PPO
ITIL INTERMEDIATE RCV
ITIL EXPERT ITIL CERTIFIED
NACS Women's Leadership Program
EC-Council ECSA CERTIFIED
EC-Council CEH CERTIFIED
EC-Council CNDA CERTIFIED
EC-Council CHFI CERTIFIED
PROJECT MANAGEMENT PROFESSIONAL PMP CERTIFICATION
CERTIFIED ASSOCIATE IN PROJECT MANAGEMENT CAPM CERTIFICATION

# Cyber Risk Management at the University of California

**Our approach to cybersecurity is structured around five pillars.**

**1. GOVERNANCE**
Enhancing governance structures helps us coordinate cybersecurity efforts.

**2. MANAGEMENT**
Strengthening risk management ensures consistent efforts across the University.

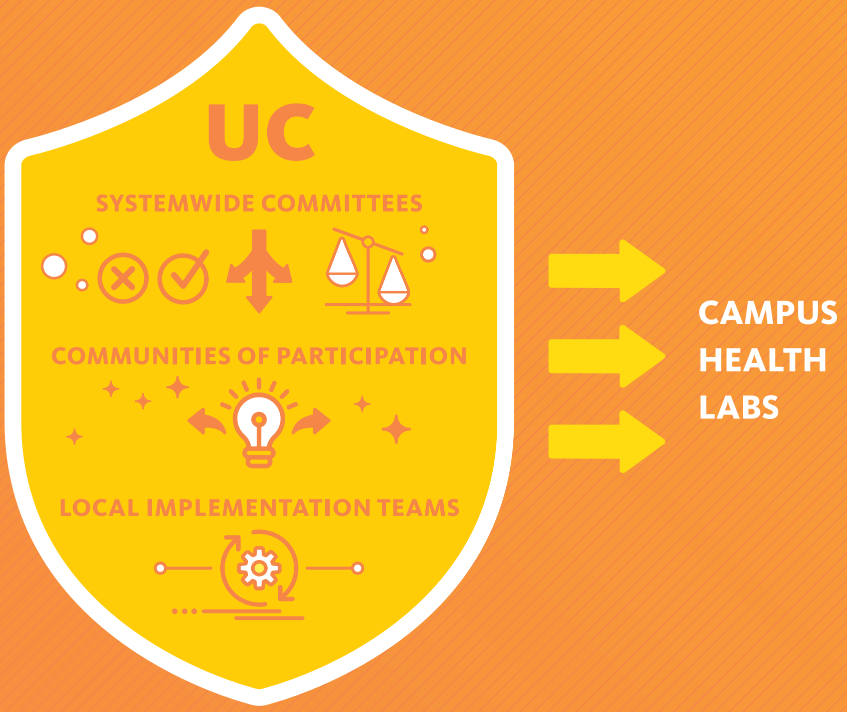
**3. TECHNOLOGY**
Adopting modern technology keeps UC one step ahead of threats.

**4. ENVIRONMENT**
Fortifying our environment through information sharing guarantees dependable protection.

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

## CYBERSECURITY IMPROVES WHEN EVERYONE WORKS TOGETHER.

Our risk governance structure includes systemwide committees, communities of participation, and local implementation teams. Together, these groups balance knowledge of systemwide requirements with proactive plans for customized protection.



UC

SYSTEMWIDE COMMITTEES

COMMUNITIES OF PARTICIPATION

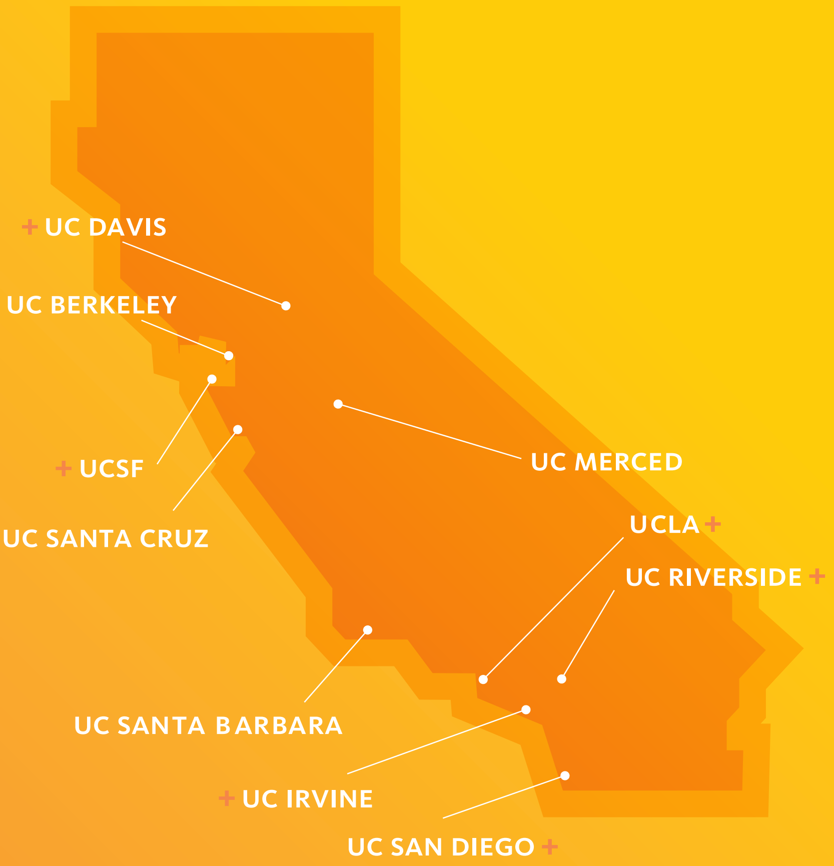
LOCAL IMPLEMENTATION TEAMS

CAMPUS

HEALTH

LABS

# UC At A Glance



+ Academic health centers

**6+** ACADEMIC HEALTH CENTERS

**TEN** CAMPUSES

**One Hundred Sixty** ACADEMIC DISCIPLINES

**THREE** NATIONAL LABORATORIES

**850** *DEGREE PROGRAMS*

**285,862** *STUDENTS*

**312,200** *EMPLOYEES*

**529,000** *JOBS SUPPORTED*

## Threat Detection and Identification (TDI)

TDI involves a variety of tools to address potential problems before they arise. We are always seeking to expand our offerings and collaborate with top experts so that we can adapt to an ever-changing landscape. TDI involves cyber threat intelligence, systemwide testing, digital threat monitoring, and much more.

**Speed is a key measurement of how security teams stay on top of threats.**

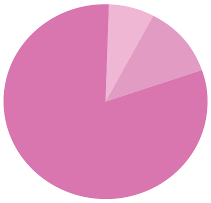
19% Average improvement in resolution time

SOURCE: hackerone, Hacker-Powered Security Report

### TDI to the Test

Some of the most serious cybersecurity events of 2021 showed us how valuable our TDI program is. During the Sunburst event, for example, TDI allowed us to complete assessments quickly and determine that no UC locations were attacked by the threat actor. Our communications tools helped us get in touch with all locations in a timely manner. We also conducted regular briefings with UC leaders and industry experts to keep everyone informed during the process.

### TDI Investment



81% Monitoring and response

12% Threat visibility expansion

7% Merging detection capabilities

SUUNTO

## Best Practice Tools and Products

The Cyber-risk Coordination Center (C3) collaborates with UC locations to enhance cybersecurity systemwide. We manage a portfolio of resources, products, and services that are available to the entire community. C3 offers technological tools, security awareness enhancement, and strategic coordination assistance needed to stay on top of the latest threats and trends in cybersecurity.

- Threat Detection and Monitoring Services
- Threat Intelligence Collection and Sharing
- Compromised Credential Notification
- Security Awareness Training Tools
- Security Operations Platforms
- Customized Learning Modules
- Breach Notification Services
- Security Risk Assessments
- Phishing Simulation Tools
- Suspicious Domain Alerts
- Forensics

## Expertise on Demand (EOD)

C3 offers services that help locations determine their level of readiness. As part of EOD, third-party experts are available to review campus incident response programs. When assistance is needed, response time is within two hours. We also provide training services and intelligence-led risk workshops. The landscape is constantly changing, and threats grow increasingly sophisticated over time. These services help us stay prepared and one step ahead.

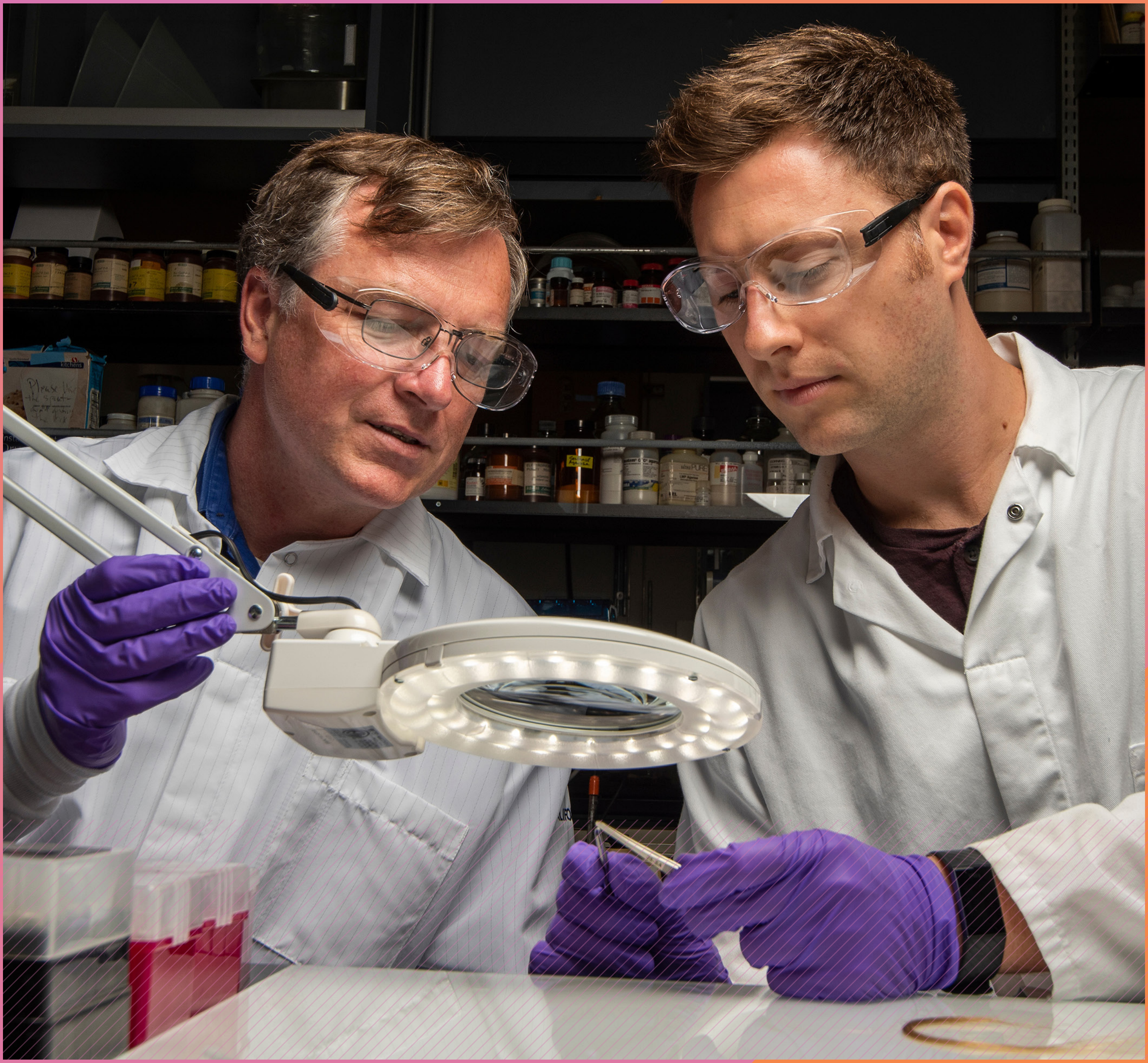
**UC is committed to best practices to mitigate the financial impacts of data breaches.**

- ➜ Invest in governance, risk management, and compliance programs
- ➜ Use data classification systems
- ➜ Invest in security orchestration, including automation, AI, and analytics
- ➜ Employ zero trust strategies to protect data and resources
- ➜ Create stress test incidence response plans to respond quickly and effectively to attacks
- ➜ Use tools to monitor and protect endpoints, especially in remote work situations

“

*Collaboration is effective because it helps us avoid costs, and, perhaps most importantly, improves problem-solving when we work together.”*

**MONTE RATZLAFF**, DIRECTOR, CYBER RISK PROGRAM, INTERIM SYSTEMWIDE CHIEF INFORMATION SECURITY OFFICER, UNIVERSITY OF CALIFORNIA OFFICE OF THE PRESIDENT



## Protecting Your Digital Self

In 2020, the Cyber Champions team dramatically increased its reach by organizing more virtual events. Building upon the success of that approach, the team developed the webinar series, *Protecting Your Digital Self*. The series was a collaboration among faculty, industry leaders, and top researchers that used an interdisciplinary approach to examine cybersecurity and its impact on real-life issues.

Cybersecurity awareness is not just about changing our passwords. It's about the intersection and impact of cybersecurity with Diversity, Equity and Inclusion (DEI). It's about protecting yourself and your communities from the damaging effects of misinformation. This series highlights how technological vulnerabilities can potentially allow an adversary to control our devices and offers many ways to mitigate that. It's all about learning to protect ourselves within the digital space.

## Cyber Champions

C3 partners with security awareness leaders across all UC locations to form a strong network of Cyber Champions. The Champions, collectively and individually by location, promote a culture of cybersecurity best practices and habits through communication and informative content. In 2021, this systemwide network of ambassadors worked diligently to create innovative outreach, webinars, trainings and awareness programs, while embedding their local perspectives.

## Cybersecurity Awareness Month

October is Cybersecurity Awareness Month. Each year, UC produces content and events to promote the highest level of organizational and personal cyber safety while also having fun. This year's events included dramatic cinematic short features, a Las Vegas mentalist, and competitive team games along with more serious expert discussions, including a UC Women's Leadership in Technology panel, cybersecurity career pathing, and cyber safety for families. The events offered something for everyone – faculty, staff and students. **#BeCyberSmart**

**UC's Information Security keeps up to date and at the cutting edge of best cybersecurity practices. We maintain a strong security posture speaking at peer conferences that set the tone for industry professionals.**

➜ UC TECH 2021: ENVISIONING THE FUTURE OF IT

➜ EDUCAUSE ANNUAL CONFERENCE 2021

➜ EDUCAUSE SECURITY PROFESSIONALS CONFERENCE (SPC)

➜ H-ISAC FALL SUMMIT: INTELLIGENCE ISLAND

➜ INFRAGARD CYBERNOW

> “
> *The work we do to share best practices is no longer just about raising awareness. It is on a different level. As threats become more and more sophisticated, we work to educate our constituents about the latest trends and how to proactively protect themselves.”*

**CECELIA FINNEY**, CYBER RISK SECURITY ANALYST,
UNIVERSITY OF CALIFORNIA OFFICE OF THE PRESIDENT

## Cyber Security Summit

Cybersecurity is a collective responsibility across the UC system. The 2021 Spring and Fall Cyber Security Summits were coordinated by C3 to offer an opportunity for hundreds of UC community members, industry experts, and higher ed stakeholders to dialogue about cyber risk management. Community collaboration allows us to build stronger, more resilient, and more adaptable protective strategies for effective response and risk reduction.

UC sets the standard for being an inclusive and diverse space for women in cybersecurity, leading by example at all levels. As in previous years, we continue our tradition of showcasing many female keynote speakers. It is always our greatest commitment to model the future of best cybersecurity practices through the perspectives and voices we amplify.

> “
> *I was so impressed with all the keynote speakers and took note that they were all women. You win the prize for walking the walk!”*
>
> **CAMILLE CRITTENDEN**, CITRIS AND THE BANATAO INSTITUTE,
> UNIVERSITY OF CALIFORNIA RESEARCH CENTER

**Cyber Summit Satisfaction and Recommendations:**

The UC Cyber Risk Program has enjoyed a consistently high satisfaction rate by its Summit attendees year-after-year, with word of mouth recommendations to colleagues increasing every year.

| | SATISFACTION | WOULD RECOMMEND |
|---|---|---|
| **FALL 2017** | 100% | 93.7% |
| **SPRING 2018** | 91% | 90% |
| **FALL 2018** | 95% | 91.5% |
| **SPRING 2019** | 91% | 92.5% |
| **FALL 2019** | 100% | 93% |
| **SPRING 2020** | 95.6% | 91.5% |
| **FALL 2020** | 89.5% | 89.5% |
| **SPRING 2021** | 92.5% | 96.3% |
| **FALL 2021** | 94% | 94.5% |

**Featured speakers included:**

**WENDY NATHER**
Head of Security, CISOs, Cisco. Wendy has more than 40 years of experience and was an Infosecurity Europe Hall of Fame inductee in 2021.

**EVA GALPERIN**
Director of Cybersecurity, Electronic Frontier Foundation

**NICOLE PERLROTH**
Award-winning cybersecurity journalist at the *New York Times*

**DERONDA DUBOSE**
Special Agent, United States Secret Service

## Information Sharing to Lower Risk

As cybersecurity professionals, we must always adapt to new threats. This means we must be flexible and effectively use the best tools available. No one knows this better than Adrian Mohuczy-Dominiak, who monitors threat intelligence and manages risk assessments for C3. Adrian ensures that our threat intelligence systems run effectively while also disseminating information system-wide. This ensures that campuses can better protect themselves using the most updated data available.

## Teamwork and Collaboration

We often say that collaboration and coordination are essential to cybersecurity work. Tools help reduce the noise so that threats are more easily detected, but human skill and intervention are still key. UCLA Health brings this into practice through their team of dedicated and diversely talented IT professionals.

The IT security landscape has changed in the last few years. A large growth in the number of remote workers and an increase in the sophistication of threats meant that a more holistic approach was in order. Traditionally, security teams are divided into blue and red teams that focus on defensive and offensive capabilities separately. This year, UCLA Health developed purple teams to increase coordination in an evolving environment.

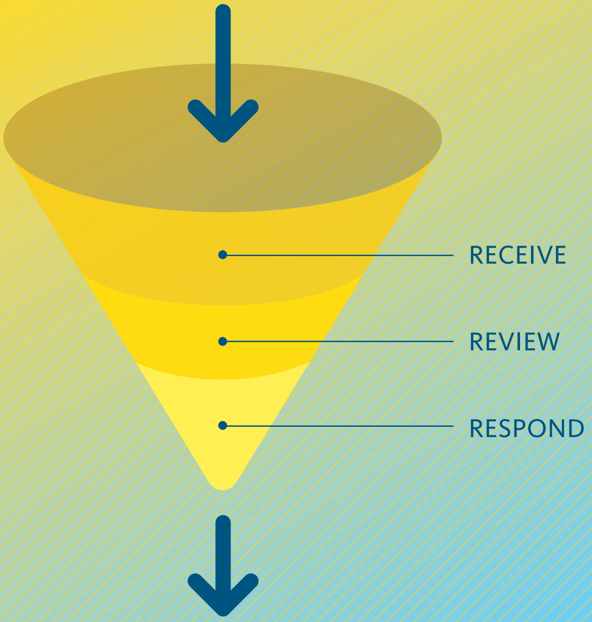
> “*We are passionate about our craft and have a deep commitment to the mission at UCLA Health. Our team brings a unique and creative vibe to their work and real value to each customer they serve. The human element is really our secret sauce.”*
>
> **JIM COLLINS**, SR. MANAGER, CYBERSECURITY, UCLA

> “*Everything is easier when you have the right people and the right connections. That’s been the bottom line for us. Our team has done an amazing job of creating and improving relationships. Now we are taking it from a reactive space to a proactive one. The purple team is a huge part of that.”*
>
> **EDGAR TIJERINO**, CHIEF INFORMATION SECURITY OFFICER, UCLA HEALTH SCIENCES

## C3 at a Glance

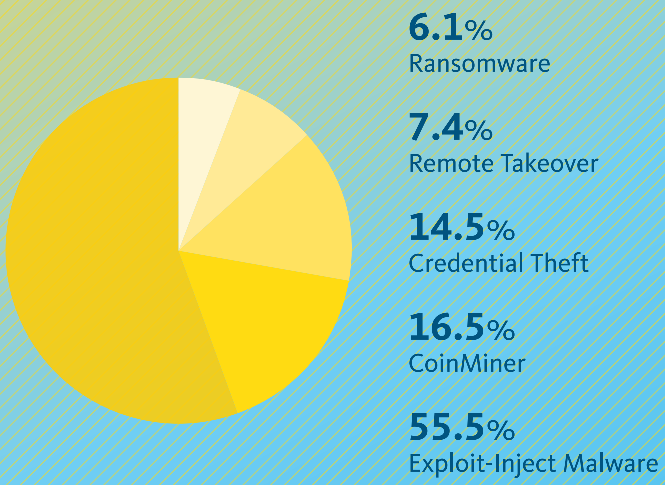
### ALERTS ANALYZED

We analyze billions of alerts. This process informs our active response to minimize threats.



### TYPES OF ALERTS

UC identified threat vectors in these categories to reduce impact.



### C3 ADVANCEMENTS IN 2021

**8X** Contract reviews for data protection increased by nearly eight times.

**DOUBLED** NEARLY DOUBLED THE QUANTITY OF NEW UC HEALTH SRAS

**78%** of faculty and staff completed Cybersecurity Awareness training

**4X** This year's Summit reach is fourfold from previous in-person events

While increasing the level of complexity of phishing campaigns, our click rate decreased by nearly **25%**

## A Self-Assessment Process to Increase Protection

Protecting the research mission of a large university isn't a task for a few IT or security professionals. It requires deeper engagement with the entire research community. At UC San Diego, this was the mantra for their Cybersecurity Certification for Research Initiative. To ensure that all research labs use effective information security practices, UC San Diego launched a self-assessment process to offer guidance for highly effective security practices. This certification process has improved the security posture for several hundred million dollars of research.

UC San Diego

## The Importance of MFA

UC Santa Barbara initiated a multifactor authentication campaign a few years ago that was integrated with their SSO. Over the past year, the program focused on administrative accounts and the process has been so successful that the total number of accounts covered is nearly 100 percent.

UC **SANTA BARBARA**

**Security at Home**

# 43%

Percent of remote tech workers reported accidentally increasing cybersecurity risks through human error.

> “
>
> *Making sure people follow best practices requires a simple approach. People are pragmatic and busy. If you give them a list of action items to prioritize, then risk is lower in a manageable way.”*
>
> **MICHAEL CORN**, CHIEF INFORMATION SECURITY OFFICER, UC SAN DIEGO

“

*We have worked to significantly reduce our attack surface. In the course of implementing MFA, you cut off the ability for people to use compromised credentials.”*

**SAM HOROWITZ**, CHIEF INFORMATION SECURITY OFFICER, UC SANTA BARBARA

## IT Recovery

This year, we completed an update of UC's IS-12 IT Recovery Policy. This policy is now modernized and designed to meet the diverse requirements of the university systemwide. It offers enhanced governance and a flexible approach to scope so that locations decide how to use the policy to fit their needs. We initiated trainings on IS-12 this fall and will have an online course available for IT Recovery professionals in 2022.

**As a system, we remain aware of changing guidelines and regulations and update our policies and strategies accordingly.**

## Using Policy to Enhance Security

At UC Berkeley this year, the CalNet Passphrase Change Project aligned systems with the updated passphrase complexity requirements laid out in the Information Security Policy, IS-3.

Berkeley
UNIVERSITY OF CALIFORNIA

The project began by implementing the new standards in our passphrase tools so that new passphrases or changes to current passphrases met the new standards. The Information Security Office then selected small cohorts and notified each via email. When the individuals in the selected cohort logged into campus systems using CalNet Authentication Service (CAS) they received a special "Password Change Required" prompt via the CAS login screen.

Each cohort had a week to comply. If an individual missed the deadline, they were automatically redirected to change their passphrase via a CAS login screen. Over a seven-month period, 80,000 passphrases were reset with only a three percent impact in tickets to help desks.

## ITPS

The Information Technology Policy and Security Community (ITPS) has over 400 members who support cybersecurity at UC. ITPS is a Systemwide CISO-supported group that works across the UC system to problem-solve through collaborative information sharing. ITPS offers constant communication through monthly meetings and a listserv that shares information about threats and vulnerabilities, peer case studies across locations, and data trends. The success of this community is the ability to find collaborative solutions to emerging cybersecurity issues in real time.

**ITPS Survey Results**

Where surveyed members found the most value in monthly meetings:

**91%**
Policy updates

**80%**
Location examples

**71%**
Regulation updates

> "
> *The monthly meetings give me ideas to bring back to my teams, help me formulate questions to ask, and just generally give good information."*
>
> *ITPS is perhaps the best UC communique I am aware of."*
>
> *Very helpful information from a trusted source."*
>
> **ITPS MEMBERS**

## Where We Stand

Cybersecurity threats are constantly evolving. A clear picture of cybersecurity helps keep us well prepared. Remote work, security AI/automation, and zero trust approaches are key areas for 2021 risk quantification and mitigation. UC educates the community about areas of risk and how to manage them.

### Risks at a Glance

**80**%
Breaches are caused by external actors

**86**%
Breaches are financially motivated

**60**%
Incidents involve hacking and compromised credentials

**36**%
Breaches involve phishing

**$4.24**M
Average cost of data breach

**$1.59**M
Average cost of lost business

### Benefits at a Glance

Good risk management investments saves organizations money and time, and builds trust

**$3.81**M
Security automation

**$2.3**M
Strong regulatory compliance

**$1.83**M
Incidence response testing

**$1.74**M
Zero trust approach

**$1.32**M
Security analytics

### Changes from 2020 to 2021

Healthcare leads with the highest costs of all industry breaches

**10**%
increase in average cost of breach

**400**K
Average increased cost of each breach

**38**%
Lost business is the largest share of breach costs

**$180**
Average cost per record of personally identifiable info

**$1.07**M
Average increase in cost for remote work breach

SOURCES: IBM Cost of a Data Breach Report 2020 and 2021, IBM Security; Data Breach Investigations Report, Verizon.

## 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