

UC Cyber Risk Program

UNIVERSITY
OF
CALIFORNIA

2020 REPORT



Welcome

Five years ago, the University of California initiated its Cyber Risk Program with one goal in mind: effective protection through a coordinated approach to risk management. Since then, we've partnered with UC locations across the system, enhancing cyber-security through collaboration and information sharing. Our work supports UC's diverse missions of education, research, healthcare, and public service and our program thrives thanks to our shared commitment to this extraordinary University.

Today, we continue to improve security as the significance of cyber risk management becomes increasingly clear. 2020 has been a year of change. Thanks to our strong program and dedicated team members, we adapted successfully to the rapidly evolving needs of our community. This year, we smoothly transformed in-person events to virtual experiences and efficiently allocated resources within budget to meet the security demands of distance learning and remote work. We also improved technologies, updated policies, managed security risk assessments, and much more.

In the following pages, you'll find details about our accomplishments and our plans for the future. As always, we recognize that our ability to support UC would not be possible without the cooperation of hundreds of people across the system. During this time of rapid adaptation, your expertise and innovation have been vital to our success. Thank you. I look forward to applying the knowledge we have gained together to the challenges of the future.




A handwritten signature in blue ink that reads "David Rusting". The signature is fluid and cursive.

David Rusting,
Systemwide Chief Information Security Officer

Table of Contents

MEET OUR TEAM MEMBERS	P 4
CYBER RISK MANAGEMENT AT UC	P 6
TOOLS AND SERVICES	P 8
SHARING BEST PRACTICES	P 12
DATA PROTECTION	P 16
POLICY	P 20
THE LANDSCAPE	P 22



“ Practicing good cybersecurity habits is more important than ever to ensure the uninterrupted delivery of UC’s mission to the people we serve.

– Michael V. Drake, MD,
President of the
University of California



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.



DAVID RUSTING	UC Chief Information Security Officer
MONTE RATZLAFF	Cyber-Risk Program Director
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.

Project Management Institution (PMI)



ISC2



Scrum Alliance



CompTIA



ISACA



SANS



Lean IT Foundation



ITIL



CWNP



Microsoft



Cisco



EC-Council



Cyber Risk Management at the University of California

Since our inception, these five pillars have guided our approach to cybersecurity.

GOVERNANCE

Enhancing governance structures helps us coordinate cybersecurity efforts.

MANAGEMENT

Strengthening risk management ensures consistent efforts across the University.

TECHNOLOGY

Adopting modern technology keeps UC one step ahead of threats.

ENVIRONMENT

Fortifying our environment through information sharing guarantees dependable protection.

CULTURE

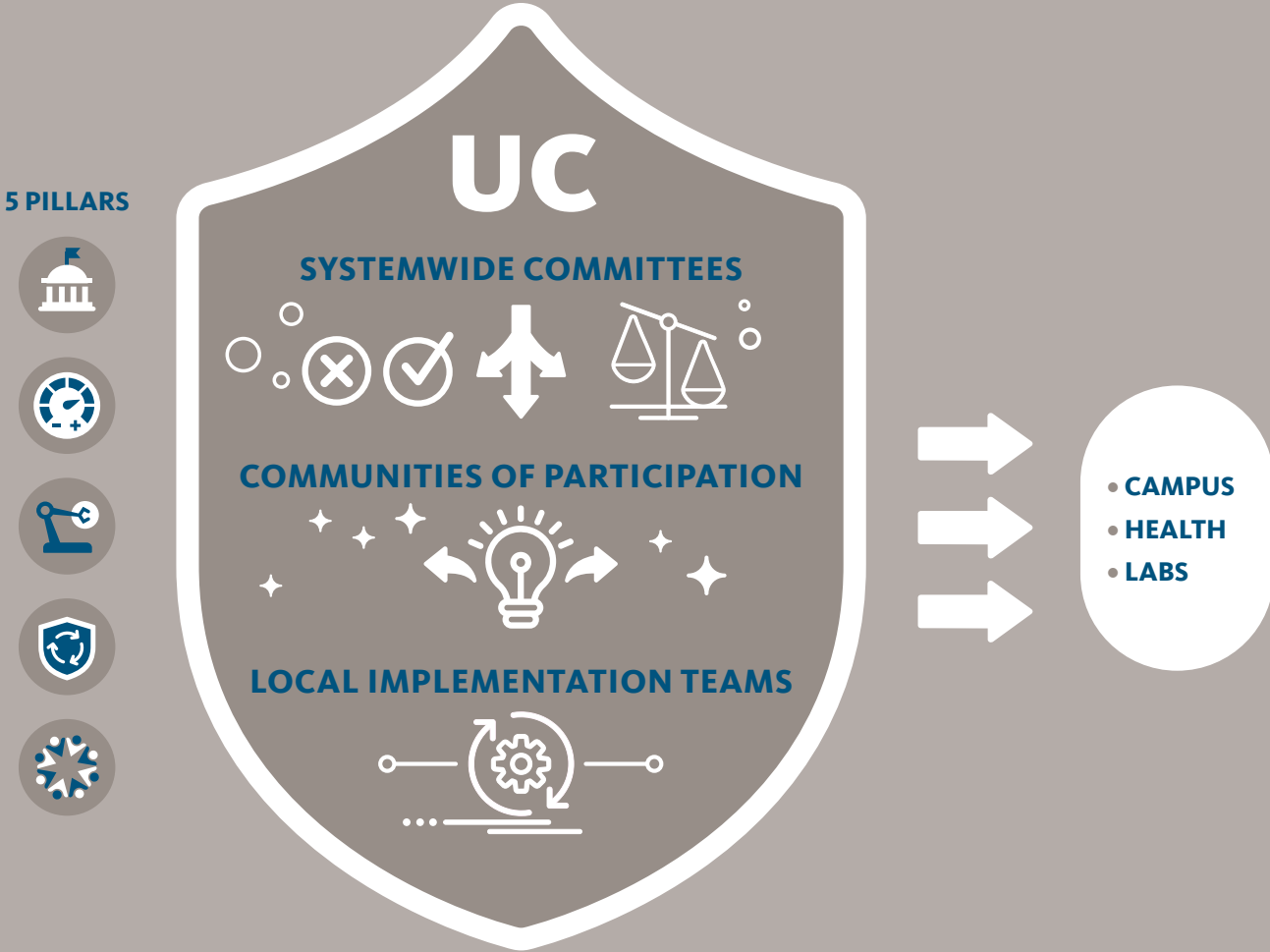
Driving culture change makes sure every stakeholder plays their part.

UC at a Glance

10 CAMPUSES	800 DEGREE PROGRAMS
6 ACADEMIC HEALTH CENTERS	280,380 STUDENTS
3 NATIONAL LABORATORIES	227,700 EMPLOYEES
160 ACADEMIC DISCIPLINES	430,000 JOBS SUPPORTED

SOURCE: universityofcalifornia.edu

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.





Enhancing Security across UC

We offer expert-guided tools and services to enhance security systemwide. Our ability to coordinate across locations allow us to protect UC's crucial missions of education, research, healthcare, and public service.



MEET MATT. Cybersecurity is a moving target. No one knows this better than Information Security Manager, Matt Linzer. When Matt joined C3 in 2018, he quickly got to work reviewing and assessing the security measures of procurement contracts for UC. As part of the collaborative process of reducing third-party risk, he vets agreements so they address security risks to UC.

Our Best Practice Tools and Products

C3 manages a large portfolio of best practice tools that help locations manage their cybersecurity, reduce risk, and respond effectively.

- ▶ 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
- ▶ Contract Risk Management



Our Contract Review Capacity Doubled in 2020

Systemwide Incident Response Coordination

We help locations enhance their incident response by offering assistance with building teams, data sharing, breach notification, and forensics. When an incident occurs, time is of the essence. Our coordinated assistance helps locations respond—and our systemwide efforts help us spot trends and lower risk.





Threat Detection and Identification (TDI)

TDI provides us with the knowledge we need to address new problems as they arise. This year, we expanded partnerships with leaders in the cybersecurity industry to give UC sites throughout the system with the most comprehensive protection available.

Cyber Threat Intelligence

The cyber threat intelligence portal provides on demand access, potential exposure information, and up-to-date risk ratings of numerous vulnerabilities every week. This new tool helps locations throughout the UC system prioritize their efforts, funneling resources where they matter most.

Systemwide Testing

C3 works tirelessly to improve our knowledge about what's working and what's not. By continuously testing UC's cybersecurity systems through simulated attacks, this pilot project will allow individual locations to test and validate controls against the tactics of known threat actors. If successful, C3 will roll out these simulated attacks across the UC system.

Threat Intelligence Enablement Manager

Integrated software tools are an incredible resource, but we also know that sometimes only a human can get the job done right. That's why it's so important that our industry partners offer a designated specialist who works with each UC location, independently and collectively, to help them get the most out of their approach.

Analyst Services (CTIAS)

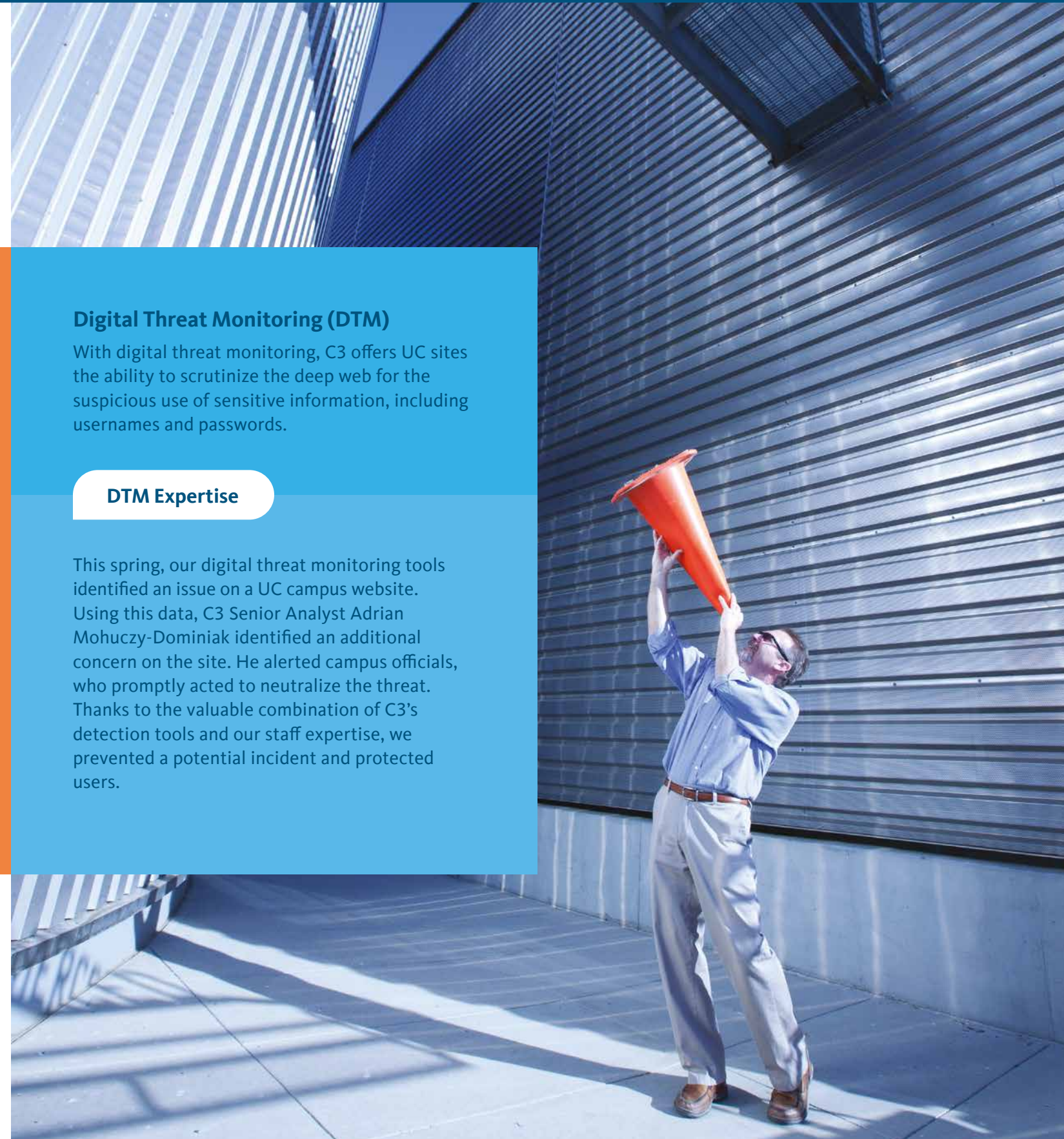
Sometimes, it helps to ask the experts. As part of our ongoing effort to provide the most up-to-date and targeted support across UC locations, C3 works with dedicated analysts who provide us with tailored guidance and advice on the most relevant cyber risks. This information lets us know what is most likely to be targeted so we can focus our monitoring efforts where it matters most.

Digital Threat Monitoring (DTM)

With digital threat monitoring, C3 offers UC sites the ability to scrutinize the deep web for the suspicious use of sensitive information, including usernames and passwords.

DTM Expertise

This spring, our digital threat monitoring tools identified an issue on a UC campus website. Using this data, C3 Senior Analyst Adrian Mohuczy-Dominiak identified an additional concern on the site. He alerted campus officials, who promptly acted to neutralize the threat. Thanks to the valuable combination of C3's detection tools and our staff expertise, we prevented a potential incident and protected users.



When breaches are contained and identified in less than 200 days, organizations save on average over a million dollars.

SOURCES: Cost of a Data Breach Report, IBM Security



Virtually Together

Cybersecurity awareness is a vital part of protecting data and resources. This year, keeping UC safe required a shift in strategy. When in-person events were no longer possible, IT professionals across the system worked to reach their audience virtually—and they increased participation in the process.

Campus Closeup

All across UC, when public safety measures changed how we worked, cybersecurity professionals looked for new ways to promote best practices that would ensure a more secure remote work environment. UC Santa Cruz's Information Technology Services, for example, coordinated with units to present crucial information and introduce community members to key security professionals who could help. Nearly 80% of UCSC units participated in their outreach program. By building relationships virtually, the office connected with almost 1000 employees and increased awareness about their services.

“Community members had new questions when their work shifted due to the pandemic. We knew we could best respond to these questions by building relationships.

– Tamara Santos, Security, Policy and Compliance Manager, UC Santa Cruz



MEET CECELIA. As a C3 Cyber-risk Security Analyst, Cecelia leads the Systemwide Security Awareness Team's efforts in developing programs and creating training that uses the latest tools for cybersecurity information. Her work ensures that all locations have the most relevant strategies. C3 fosters a robust cybersecurity culture thanks to these remarkable resources and facilitated information sharing.

“They say necessity is the mother of invention. It's true—that's exactly how we moved NCSAM to the next level. By building a centralized platform full of options that we could share systemwide, we increased participation and engagement. It also set the stage for more exciting events in the future.

– Cecelia Finney, Cyber Risk Security Analyst, C3

National Cybersecurity Awareness Month (NCSAM)

C3 prepared for NCSAM this October by developing activities and resources for every location. Thanks to the virtual nature of all our events, our ability to collaborate was greater than ever.

We created a centralized portal that allowed community members to register for events at any location. We had a variety of new options, including games and movies related to cybersecurity and a popular cyber escape room. We also provided customized Zoom backgrounds.



C3 Advancements in 2020

NCSAM webinars available systemwide increased nearly tenfold



Over 500,000 trainings completed



Summit attendance nearly quadrupled





Our Biannual Cyber Security Summit

C3 coordinates the biannual UC Cyber Security Summit, which promotes collaboration and coordination among faculty and staff across the UC system, as well as the California State University and the community colleges. This spring, we had less than a month to convert our in-person event to a virtual one due to the global pandemic. Not only did we pull it off, we created an exemplary event with over 400 attendees, many of whom said it was the most successful and engaging virtual summit they had experienced.

In fact, the rapid transition turned out to be a valuable learning experience. We learned how to increase engagement and create an even stronger cybersecurity culture. For example, our team added live music, offered games, prizes, and other rewards for participation, and made sure that all attendees had opportunities for networking. Though our transition was quick and demanding at first, we gained valuable knowledge that will inform our plans for future summits, both in-person and virtual.



MEET WENDY. As the Cyber-Risk Coordination Center Manager, Wendy Rager ensures the success of our biannual Cyber Security Summits. She brings her impressive experience in IT management to her work, guaranteeing that the events foster connection and enhance security, whether online or in-person.

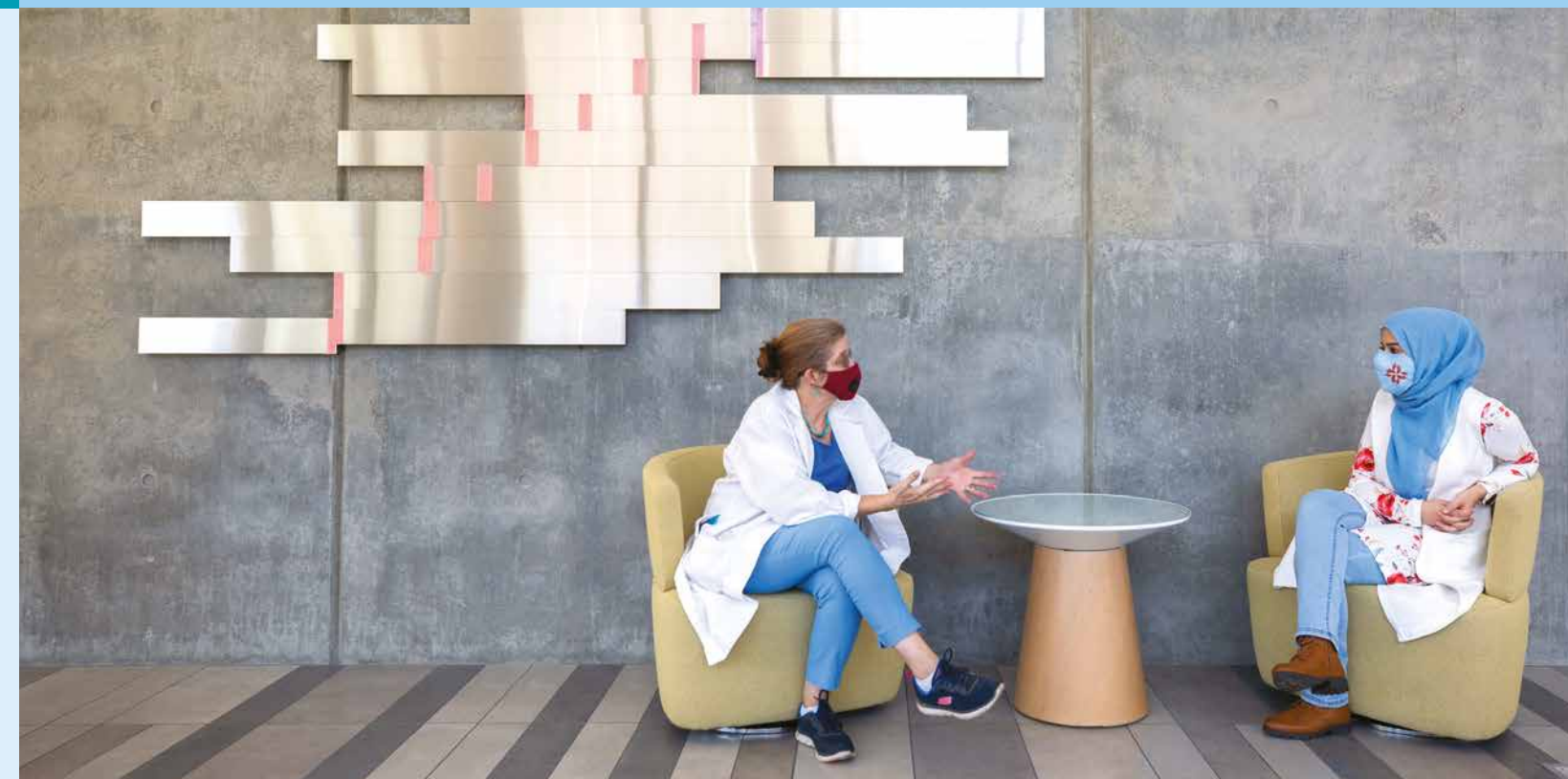
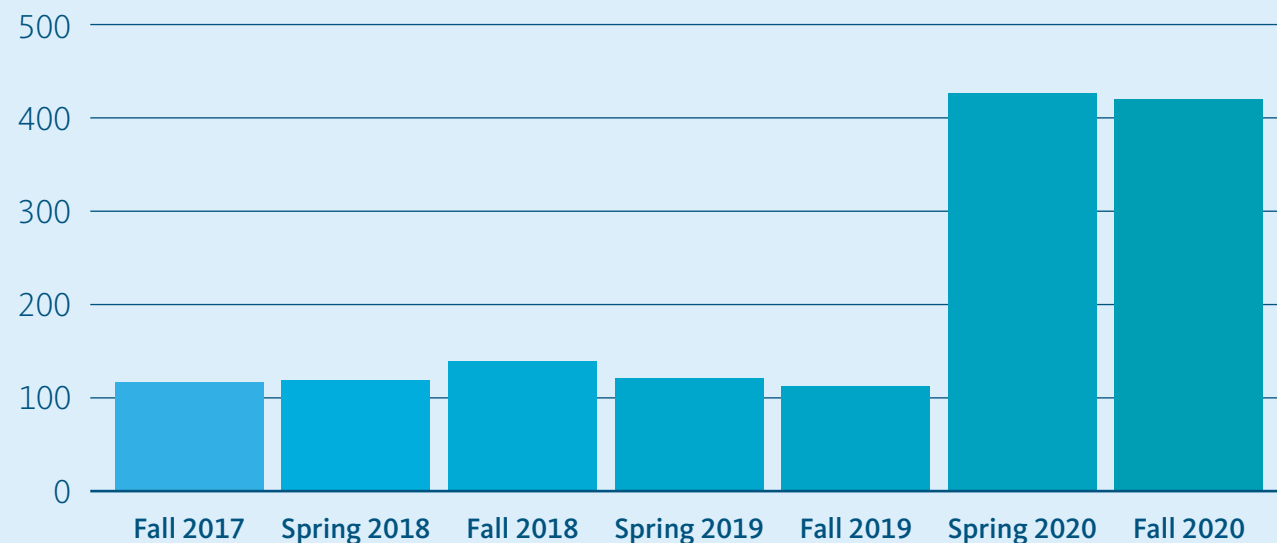
Building Relationships

In addition to hosting two UC systemwide summits per year, C3 team members learn and share information at conferences around the nation. This year, our representatives discussed multiple topics, including ensuring security in healthcare, reducing risk, building resilience, and educating future leaders in cybersecurity.

2020 UC Presentations

Healthcare Innovation Cyber Security Forum	San Diego	February 5
Marsh North American Annual Conference	Virtual	March 17
EDUCAUSE Security Professionals Conference	Virtual	June 2
State of California Cybersecurity Industry Convening	Virtual	August 2
EDUCAUSE Webinar	Virtual	August 4
UC Tech 2020: Envisioning the Future of IT	Virtual	August 11
EDUCAUSE 2020	Virtual	October 27
EDUCAUSE Cybersecurity Experience Summit 2020	Virtual	November 5

Attendee Trend





Adaptive Risk Management

Reducing cyber risk is a crucial endeavor for any organization, and especially for workers, researchers, and patients during a global pandemic. This year, we continued our valuable Security Risk Assessment process, enhanced security for health-related researchers, and adapted to better protect data and devices in remote environments.

Endpoint Security Monitoring

Endpoint security protection has always been a crucial part of cyber-risk management at UC, but the pandemic made this tool more important than ever. When COVID-19 scattered members of the UC system to worksites all over the world, C3 responded by increasing protection for users wherever they worked. Locations had access to vital endpoint security software free of charge thanks to C3's efficient realignment of resources within budget.

Campus Closeup

Tolgay Kizilelma, Chief Information Security Officer at the University of California Merced, knew that a focus on endpoint security management was crucial from the time he began his work at the university. "We need to protect ourselves from thousands of threat actors," says Kizilelma. "In the cycle of how attacks start, the device is often the beginning. This is why endpoint security is so valuable."

This type of protection was, of course, not new at the beginning of the pandemic, but C3's prompt decision to offer endpoint security management software to all locations free of charge created a new and better environment across the system. Kizilelma notes that this solution helped UC campuses like Merced in two ways: first, it emphasized the value of the approach; and secondly, it ensured consistent protection systemwide so IT professionals had more data and fewer gaps in coverage.

Security at Home

In one survey of remote tech employees, 43% reported making a mistake that increased cybersecurity risk.



Security Risk Assessments (SRAs)

Security Risk Assessments ensure patient privacy and HIPAA compliance. C3 manages SRAs for UC Health Community Connect Partners.

"We really appreciate C3's direction and guidance during the SRA process."

– UCLA Health

Avoiding Phishing Scams

Phishing continues to pose a significant threat to cybersecurity at UC as cyber attacks increase in sophistication and volume every year. In fact, most organizations experience at least one successful phishing attack per year. That's why C3 coordinated several phishing campaigns for UC Health this year, keeping health and identity information safe and secure. We use some of the world's leading phishing simulation tools to educate users, find vulnerabilities, and protect the UC system from threats as they emerge.





UC Health

UC Health's data security has become more important than ever as researchers and clinicians learn how the coronavirus impacts different populations, communities, and individuals. We support UC Health researchers who offer cutting edge treatment and solutions. Through our secure data warehousing system, C3 helped researchers learn about and respond to the COVID-19 pandemic as it unfolded.



MEET MONTE. Monte Ratzlaff works with UC leaders to establish cyber risk strategic plans and objectives. When UC Health launched its Center for Data-driven Insights and Innovation (CDI2), Monte's role as the systemwide Cyber Risk Program Director made him a leader in efforts to protect the sensitive health information of millions of patients across the UC system.

Campus Closeup

Direct Outreach to Enhance Security

The sudden shift to virtual communications in early spring 2020 meant that UC cybersecurity professionals had to act quickly to increase awareness about new and ongoing risks. The UC Berkeley Information Security Office recognized the need to add additional security protections, not just for general work-from-home risks, but for critical COVID-19 research as well. They promoted their restricted VPN and high-security firewall services for systems working with high-value data and, like Merced, leveraged UC systemwide endpoint security monitoring software. However, the biggest impact came through direct outreach.

The Berkeley office partnered with the Vice Chancellor for Research and Research IT to present to an audience of over 300 researchers and support staff. After opening remarks from senior leadership, the presenters provided specific information on new threats, the most common types of attacks, the tools available to help researchers protect their data, and how to reach out for assistance. This networking provoked several researchers to seek cybersecurity assistance and therefore improve their resiliency against ransomware and other threats.

“ We knew we needed to connect on a personal level to ensure researchers were aware of the threats targeting them and the tools available to keep their data secure.

– Allison Henry, UC Berkeley CISO



Improve the success rate for publication and funding opportunities

Facilitate data management, use, and reuse



Cyber Champions

Cyber Champions create a culture of awareness by promoting cybersecurity best practices at their respective locations. C3 partners with campuses in their efforts to build and enhance their champion programs. In 2020, representatives from every campus participated. We focused our efforts on online resources, providing champions the opportunity to participate in a variety of optional trainings.

“ Cybersecurity is an ongoing problem because we are always under threat. Having opportunities for collaboration and resource sharing through C3 is vital to our success.

– Kip Bates, Associate Chief Information Security Officer, UC Santa Barbara



Connecting Globally

UC's strategies, tools, and efforts aren't only making things safer here at home, they're shaping the landscape of cybersecurity around the nation—and the world. Our IT Policy Office helps structure UC's response to state and federal regulations. It also works with agencies at the local, state, and federal level to set cybersecurity standards and educate leaders on how to protect data and minimize threats. We share threat intelligence and partner with a variety of organizations to gain valuable insight into the latest trends in cybercrime. From advising the government on the National Defense Authorization Act to providing detailed policy tools, we make sure UC is connected to the wider world of cybersecurity.

Intelligence Sharing

We improve cybersecurity by partnering with:

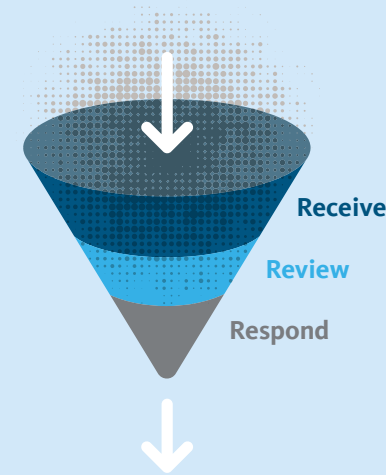
- ▶ (H-ISAC) Health Information Sharing and Analysis Center
- ▶ (MS-ISAC) Multi-State Information Sharing and Analysis Center
- ▶ (REN-ISAC) Research Education Networking Information Sharing and Analysis Center
- ▶ (CAL-CSIC) California Cybersecurity Integration Center
- ▶ Cyber Crimes Task Force
- ▶ Government Agencies
- ▶ Multinational companies

Guidelines at a Glance

- ▶ This year, we created new guidance for travelers, helping UC community members protect themselves from common threats when visiting less protected environments.
- ▶ Robert Smith, Systemwide IT Policy Director, offered an educational webinar on using Appendix Data Security to manage supply chain risk.
- ▶ The Information Technology Policy and Security Committee (ITPS), with over 400 members, met several times throughout the year, discussing vital topics, such as data classification, endpoint protection, COVID-19 communication practices, cyber insurance, and much more.
- ▶ Our policy team is revising and updating IS-12, the UC systemwide policy on IT Recovery to better respond to our evolving security landscape.

C3 At a Glance

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



Campus Closeup

From College to Career

Promoting a culture of cybersecurity involves not only assisting employees, researchers, care providers, and educators—it's also about preparing students to be leaders in the field of cybersecurity. UC Riverside's Chief Information Security Officer (CISO), Dewart Kramer, for example, has set a new direction for information security at UCR, which includes providing invaluable work experience to students. "As those in information security know, students play an essential role in protecting campus data and sensitive user information on the front end," explains Kramer. "It makes sense to involve students currently earning their degrees in various computer science fields in the important back-end work, too. This also provides crucial work experience in a highly competitive field." Students who get valuable hands-on experience not only promote cybersecurity in their campus community, they also develop vital skills to help us meet the challenges of an ever-changing field.

"I am grateful for the real-world experience ITS has given me and feel it is already paying off. I recently secured an information security internship and, after a few days, it was evident that my knowledge exceeded that of my fellow interns."

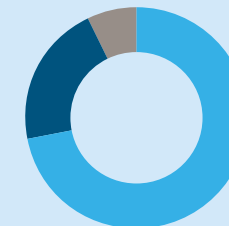
— Juan Barrientos, Student, UC Riverside

Budget Breakdown

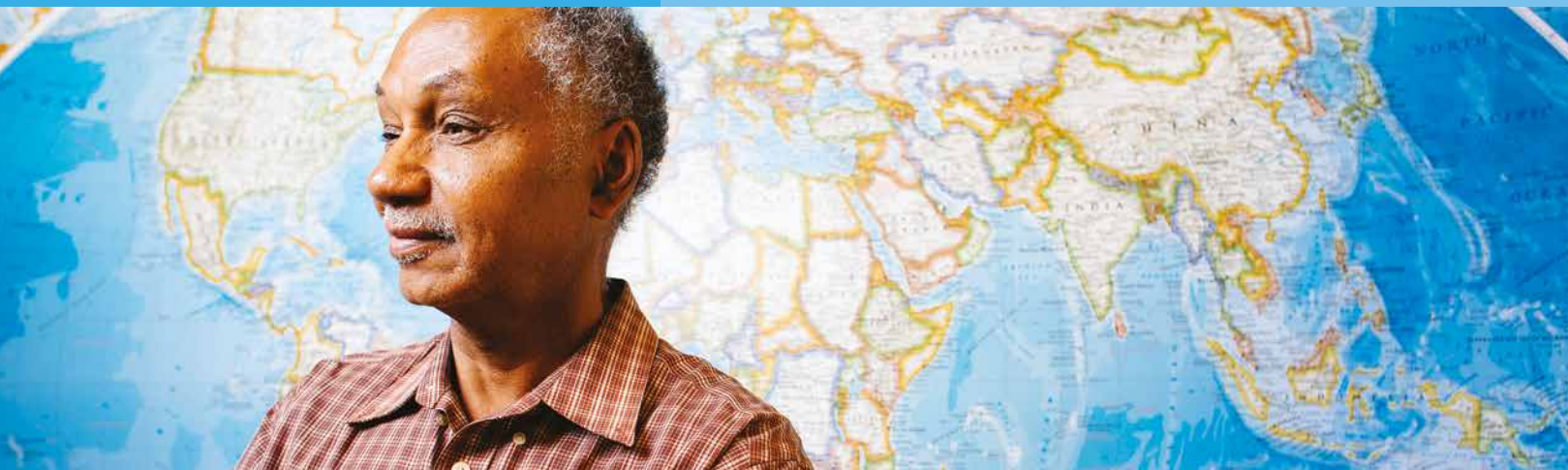
+ \$2.1M (Salary/Benefits/Insurance)
 + \$8.3M (TDI)
 + \$0.2M (Misc)

\$10.6M Overall Spend

TDI Investment



72% Monitoring and Response
 21% Threat Visibility Expansion
 7% Emerging Detection Capabilities



The Landscape

Cybersecurity threats evolve over time. As they become more sophisticated, we work to stay one step ahead. This is why we educate our community members about the field and the benefits of risk management.



Risks at a Glance

- 70%** Breaches that involve external actors
- 45%** Breaches that include hacking
- 58%** Victims that had personal data compromised
- 86%** Breaches are financially motivated
- 52%** Breaches caused by a malicious attack
- 1.52M** Average cost of lost business
- 3.86M** Average cost of a data breach

Benefits at a Glance

Cybersecurity risk management is cost effective. It saves, on average, the following amount for each of these actions.

Incident Response Testing

\$295K

Employee Training

\$238K

Data Loss Prevention

\$164M

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



