

# UC Cyber Risk Program

2019 REPORT

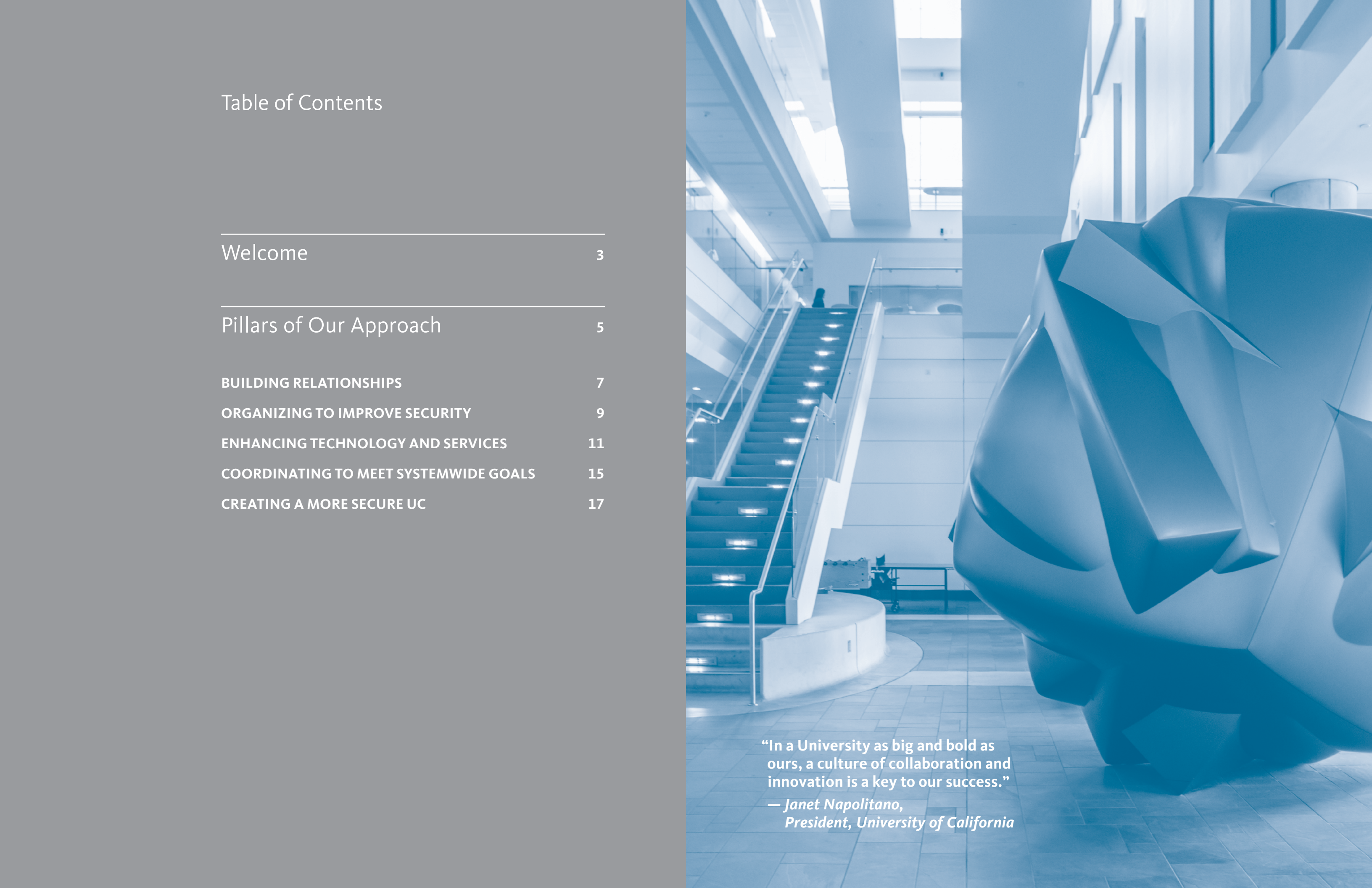


**UNIVERSITY  
OF  
CALIFORNIA**

## Table of Contents

---

Welcome	3
<hr/>	
Pillars of Our Approach	5
<b>BUILDING RELATIONSHIPS</b>	7
<b>ORGANIZING TO IMPROVE SECURITY</b>	9
<b>ENHANCING TECHNOLOGY AND SERVICES</b>	11
<b>COORDINATING TO MEET SYSTEMWIDE GOALS</b>	15
<b>CREATING A MORE SECURE UC</b>	17



**“In a University as big and bold as ours, a culture of collaboration and innovation is a key to our success.”**  
— *Janet Napolitano,*  
*President, University of California*

## Welcome



When the University of California initiated its Cyber Risk Program in 2015, our goal was to build a consistent and coordinated approach to risk management. Over the past four years, we have done this by working together with UC locations across the system to support UC's diverse missions of education, research, healthcare, and public service. Our shared commitment to protecting this wonderful institution continues to motivate our work today.

2019 was a dynamic year for the UC Cyber Risk Program. We successfully deployed a phishing simulation solution for all campuses and health systems; we were invited to present on our program to cyber insurance specialists in London; and we enhanced our threat detection services to monitor the dark web for risks to UC. Our program also organized summits, created educational tools, improved technologies, coordinated incident response, managed security risk assessments, and much more.

In the following pages, you'll find details about our accomplishments and our plans for the future. Our advances over the past four years would not have been possible without the collaboration of hundreds of people across the UC system. I thank all of you who have joined us on this journey and who will continue to work with us as we support UC in the years to come.

David Rusting  
*UC Chief Information Security Officer*



### OUR MISSION

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

## Pillars of Our Approach

These pillars of cyber-risk reduction guide the work we do.



### 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.



## BUILDING RELATIONSHIPS

Even in our technologically advanced world, nothing can replace the value of face-to-face conversations. The UC Cyber Risk Program builds relationships, learns from others, and shares our expertise by traveling to conferences and hosting a biannual summit.

### Conferences

In 2019, members of our team traveled far and wide to share our expertise.

HIMSS NorCal Chapter Conference Sacramento, CA January 24	Corporation for Education Network Initiatives Annual Conference La Jolla, CA March 18-20
EDUCAUSE Security Professionals Conference Chicago, IL May 13-15	UC Risk Summit Anaheim, CA May 30-31
UC Davis Information Security Symposium Davis, CA June 18-19	UCTech Conference Santa Barbara, CA July 17
EDUCAUSE Annual Conference Chicago, IL October 14-17	UC Ethics, Compliance, and Audit Symposium Newport Beach, CA October 28-30

### Cyber Security Summits

Risk management improves when people work together. This is why C3 hosts a Cyber Security Summit every spring and fall at a different UC campus. Attendees leverage collective skills, share ideas, and meet new people. This year, key stakeholders and industry leaders met at UC San Francisco in April and UC Santa Barbara in October to discuss the latest ideas and strategies for enhancing cybersecurity.



**“The UC cybersecurity community achieves an unprecedented level of collaboration systemwide.”**

— *Summit Attendee*



## ORGANIZING TO IMPROVE SECURITY

Our program's targeted committees help us meet the diverse needs of the entire UC system. We also coordinate with government and industry professionals worldwide.

### At UC

UC's risk governance structure includes system-wide committees, communities of participation, and local implementation teams.

#### SYSTEMWIDE COMMITTEES

- (CRGC) Cyber-Risk Governance Committee
- (ITLC) IT Leadership Committee
- (ITSC) IT Security Committee
- (ECAS) Ethics, Compliance, and Audit Services

#### COMMITTEES OF PARTICIPATION

- (UCSIRC) UC Security Incident Response Coordination
- (GERI) General Counsel, Ethics and Compliance, Risk and IT Committee
- (ITPS) IT Policy and Security Committee

#### LOCAL IMPLEMENTATION TEAMS

- (UC Health LSfV) Leveraging Scale for Value
- (CDI2) Center for Data Driven Insights and Innovations
- (UCACC) University Committee on Academic Computing and Communications



### Worldwide

Cybercrime is a problem worldwide. UC therefore partners with a wide variety of organizations to share threat intelligence and gain valuable insight.

- (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-SIC) California Cybersecurity Integration Center
- Cyber Crimes Task Force
- Homeland Security
- FBI
- Secret Service
- Multinational companies

In 2019, UC worked closely with H-ISAC to select the best content for its spring summit, which draws over 600 healthcare and pharmaceutical security professionals.





## ENHANCING TECHNOLOGY AND SERVICES

Cybersecurity protection improves thanks to planned and coordinated efforts across an entire system. Our program offers multiple services that enhance security, including managed assessments and customizable training modules.

### Systemwide Incident Response Coordination

We help locations enhance their incident response by offering assistance with team building, data sharing, breach notification, and forensics. Location incident reporting also helps us coordinate effectively. Our systemwide approach allows us to spot trends, identify threats, and lower risk.

### Security Risk Assessments

Electronic medical records improve health because they provide easily accessible information about patients across the continuum of care. The University of California Health System makes the use of electronic records easier by offering **UC Health Community Connect Partners** access to their advanced healthcare records system. C3 manages Security Risk Assessments (SRAs) for new affiliates. These assessments ensure HIPAA compliance and keep patient records secure.

### Incident Reporting

C3 helped a UC campus protect their accounts through incident reporting. The campus notified us of suspicious activity and we acted quickly. Thanks to our specialized resources and key security tools, we determined that foreign actors were selling data on the dark web that might impact UC. Our coordinated efforts kept over 85k accounts protected from harm.

2X

### Demand Doubled

The number of new **UC Health Community Connect Partners** doubled in 2019.





## ENHANCING TECHNOLOGY AND SERVICES (CONT.)

### Toolkit: A Portfolio of Best Practice Tools and Services

C3 manages a large portfolio of best practice tools that help locations manage their cybersecurity, reduce risk, and respond effectively. The C3 toolkit is full of resources locations can use to enhance their cybersecurity.

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

### TOOLKIT EXAMPLES

#### Threat Detection and Identification (TDI)

Threat detection tools are vital to our work. They help us focus our response efforts and prepare for a changing threat landscape.

This year, TDI pinpointed roughly 75,000 actionable alerts in a haystack of 100 billion events.



#### Phishing Simulation

Our program uses sophisticated phishing simulation tools in order to keep users vigilant. Information from campaigns often serves as a teachable moment and helps locations customize their training, too.

In September 2019, UC organized 16 campaigns across 9 locations. Our click rate improved from the prior year, reaching a level below the industry standard for healthcare and education.







## COORDINATING TO MEET SYSTEMWIDE GOALS

UC's Cyber Risk Program develops policies that establish baseline requirements and allow locations the flexibility to meet their specific needs. These coordinated efforts ensure a cohesive approach to security that can adapt to meet the demands of a large organization in a changing threat landscape.

### Ensuring Best Practices

#### IS-3 STANDARDS AND GUIDES

This year, we approved new standards and guides that support our systemwide information security policy, IS-3. These documents cover crucial topics, such as account access, event logging, software configuration, and key encryption. Easily updated, they ensure that baseline requirements keep up with changing needs.

#### CONTRACTUAL RISK MANAGEMENT

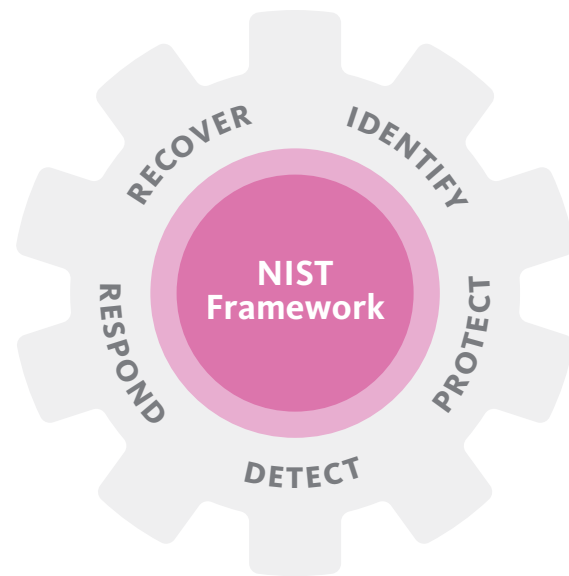
Our program reviews all systemwide contracts to ensure cybersecurity best practices. In 2019, we reviewed nearly fifty contracts on a variety of topics, including payment processing, medical benefits, and human resource solutions.

#### APPENDIX DATA SECURITY

We updated the contract that establishes crucial guidelines for secure supplier agreements, Appendix Data Security (DS). This spring, hundreds of employees met for in-person trainings on how to use the Appendix.

### Cyber Insurance

Cyber insurance covers the cost of incident response services and makes us better prepared to respond when incidents occur. This spring, cyber insurance underwriters invited UC's CISO to London to present on our program's impressive accomplishments.



**“The Appendix DS training was great. It was a pleasure to learn information that I can use as my department grows and strengthens its security program.”**

**— Training Attendee**





## CREATING A MORE SECURE UC

When all UC stakeholders understand the risks of our technologically advanced world, they can better react and prepare for them. C3 enhances security awareness through a wide range of tools and services, including videos, posters, games, and training applications with customizable modules that target specific topics or workgroups.

### Sharing Effective Strategies

The **Systemwide Security Awareness Workgroup** is a collection of security awareness managers and professionals at UC who organize events and programs at their respective campuses. The **Student Security Awareness Workgroup** serves a similar purpose and focuses on topics and materials that target student users in particular. Both workgroups discuss location-level initiatives and share information about effective tactics that enhance security.

### Learning Together

October is **National Cybersecurity Awareness Month** and multiple events occur across UC. This year, Dr. Gigi Johnson of UCLA's Center for Music Innovation at the Herb Alpert School of Music spoke to staff at the University of California Office of the President. She shared information about how even popular uses of technology, like creating playlists, leave us open to being tracked and influenced when making major life decisions.



### Making Conversation

UC San Diego asked community members to describe their thoughts on information security in **six words**. Thousands of people responded, sparking a campus-wide discussion about best practices. The campaign has inspired other campuses to follow suit.

6  
WORDS

SECURE. ALERT.  
FIREWALL.  
EXTORT. THREAT.  
YIELD.

SECURE OUR  
DATA, EASE OUR  
MINDS.

### Improving through Teamwork

**Cyber Champions** create a culture of awareness by promoting cybersecurity best practices at their respective location. C3 partners with campuses to create systemwide resources and we support campuses as they begin and enhance their programs.



This December, we gathered at UCSF to celebrate the work of UC's Cyber Champions. These dedicated individuals advocate for security awareness, helping all community members play their part in building a more secure future.



## WANT TO KNOW MORE?

### CONTACT US

DAVID RUSTING

CHIEF INFORMATION SECURITY OFFICER, UNIVERSITY OF CALIFORNIA  
UC CYBER RISK PROGRAM, OFFICE OF THE PRESIDENT

[C3@UCOP.EDU](mailto:C3@UCOP.EDU)