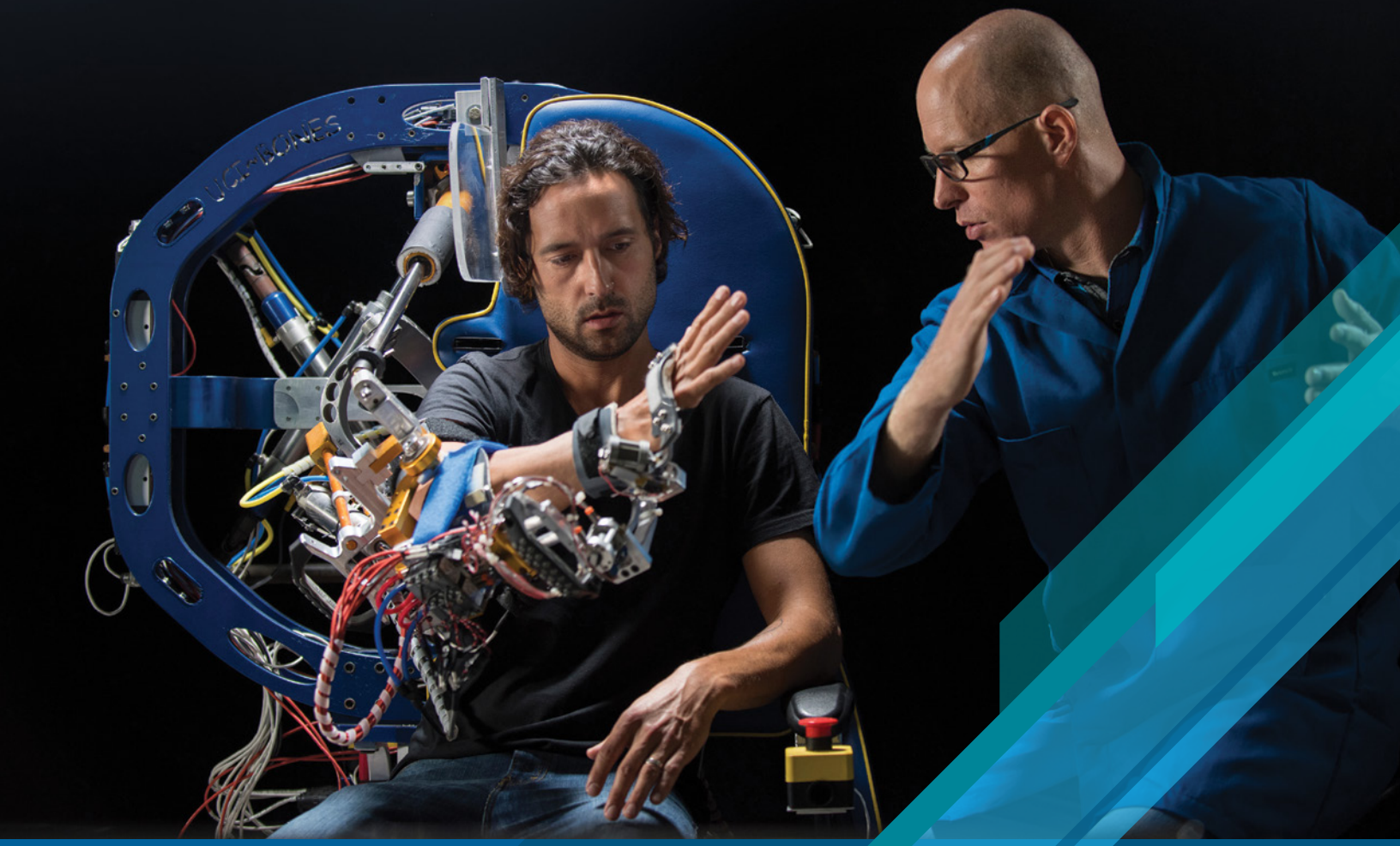
UC Cyber Risk Program

REPORT 2022



UNIVERSITY OF CALIFORNIA

TABLE OF CONTENTS

2 Meet Our Team Members
3 Team Members' Certifications
4 Cyber Risk Management at UC
5 UC at a Glance
6 UC Security Leadership
8 Tools and Services
12 Sharing Best Practices
18 Protection Across the System
24 Guidelines and Strategies
26 Campus Spotlights
28 The Landscape

Welcome

The University of California's Cyber Risk Program has matured since its establishment in 2015, growing through cooperation and partnership. We seek to develop a cybersecurity mindset that lives not just within IT Security, but the whole gamut of staff, faculty, and students. We work to provide systemwide support, and we recognize that people are at the heart of the challenges we face.

The human factor might play the most significant role in cybersecurity events, as it powers vigilance and innovation, allowing us to meet new and rising threats head-on. You'll find that this report on the program's 2022 accomplishments focuses as much on people as technology, highlighting successes in education, collaboration, policy, and process. Together we've rolled out updated and new training, created broad awareness of best practices and tools for systemwide cybersecurity health, and grown as a community.

The Cyber Risk Program truly depends on the contributions of many people across the UC system who work to create inclusive, accessible, and impactful cybersecurity. I look forward to the continued success of this community; together we flourish.

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

> *Effective cybersecurity is as much about the sociological systems as it is about the technological systems. It is as much about transforming habits, hearts, and minds as it is keeping up to date with the latest tools and practices.*
>
> **VAN WILLIAMS, Vice President of IT and Chief Information Officer, 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.

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
Systemwide Cyber Champion Team Leader

FARROKH KHODADADI
Cyber Risk Technical Security Analyst

JACKIE PORTER
Cyber Risk Project Coordinator

Team Members' Certifications

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

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

Cyber Risk Management at UC

Our approach to cybersecurity is structured around five pillars.

1. GOVERNANCE
Enhancing gover nance structures helps us coordinate cybersecurity efforts.

2. MANAGEMENT
Strengthening risk management ensures consistent efforts across the UC.

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

4. ENVIRONMENT
Fortifying our environment through information sharing guarantees depend able protection.

5. 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
- → IT Security Committee
- → Ethics, Compliance, and Audit Services
- → University Committee on Academic Computing and Communications

Communities of participation:

- → UC Security Incident Response Coordination
- → General Counsel, Ethics and Compliance, Risk and IT Committee
- → IT Policy and Security

Local implementaion 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

UC Security Leadership

Meet our Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs). Established or new to the University of California, our leadership is committed to reducing UC's cyber risk.

CAMPUS	CIOs	CISOs
Agriculture and Natural Resources	Sree Mada	Jaki Hsieh Wojan
Berkeley	Jenn Stringer	Allison Henry
Davis	Viji Murali	Cheryl Washington
Davis Medical Center	Ashish Atreja	Nicholas Borton
Irvine	Kian Colestock	Josh Drummond
Irvine Medical Center	Scott Joslyn	Gabriel Gracia
Lawrence Berkeley Lab	Adam Stone	Jay Krous
Los Angeles	Lucy Avetisyan	David Shaw
Los Angeles Medical Center	Ellen Pollack	Edgar Tijerino
Merced	Nick Dugan	Jackson Muhirwe
Office of the President	Molly Greek	April Sather
Riverside	Matthew Gunkel	Dewight Kramer
Riverside School of Medicine	Simon Linwood	Matthew Summerville
San Diego	Vince Kellen	Michael Corn
San Diego Medical Center	Joshua Glandorf	Scott Currie
San Francisco	Joe Bengfort	Patrick Phelan
San Francisco Medical Center	Joe Bengfort	Patrick Phelan
Santa Barbara	Josh Bright	Emilio Valente
Santa Cruz	Aisha Jackson	Brian Hall
Systemwide	Van Williams	Monte Ratzlaff (interim)

In my first 100 days as CISO, we fully implemented our Information Security Management Plan (ISMP), which is an IS-3 requirement.

JACKSON MUHIRWE, CISO, University of California, Merced

Threat Detection and Identification (TDI) Program

The TDI program leverages systemwide expertise across UC using a common platform to enable coordinated responses to potential cybersecurity events. It involves cyber threat intelligence, system-wide testing, digital threat monitoring, and analyst services. The TDI program means we can have a faster response time and threat remediation.

The TDI program capabilities lead to awareness of potential threats, network and endpoint visibility, and a better understanding of threats and vulnera-bilities. Meeting the TDI program objectives leads to curated threat intelligence. It also means that people are better prepared for incident response engagement and increasingly educated so they can operate with a cybersecurity mindset.

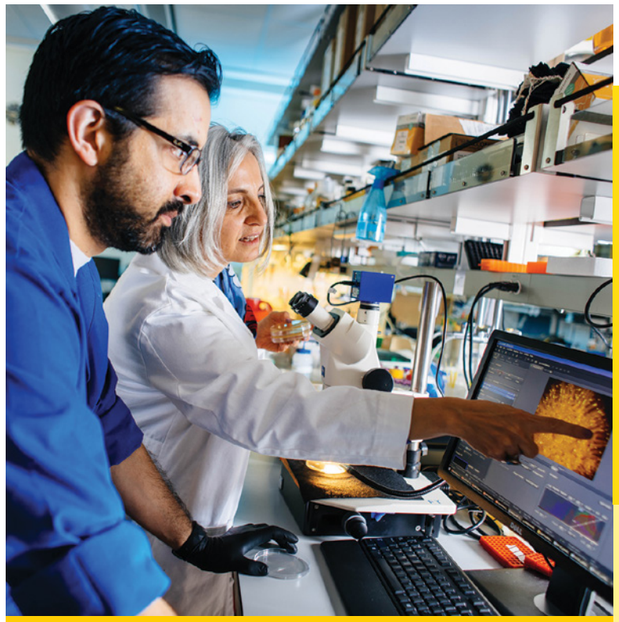
TDI program objectives:

- → Systemwide tool manages cybersecurity risk
- → Same view of security
- → Spot bad actors consistently
- → Respond quickly and uniformly

Achieving our TDI objectives leads to awareness of potential threats, network and endpoint visibility, and better understanding of threats and vulnerabil-ities. This is thanks to curated threat intelligence. It also means that people are better prepared for incident response engagement and increasingly educated so they can operate in a cybersecurity mindset.

Digital Threat Monitoring

Digital Threat Monitoring enables us to look at high-risk attacks from the deep and dark web, as well as attack campaigns. The tools we used help us narrow our effort to the highest possible threats. In 2022, we removed almost 98% of the noise.



TDI INVESTMENT

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

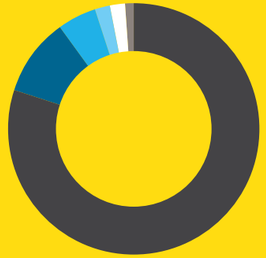
87%
Monitoring and Response

10.9%
Emerging Detection Capabilities

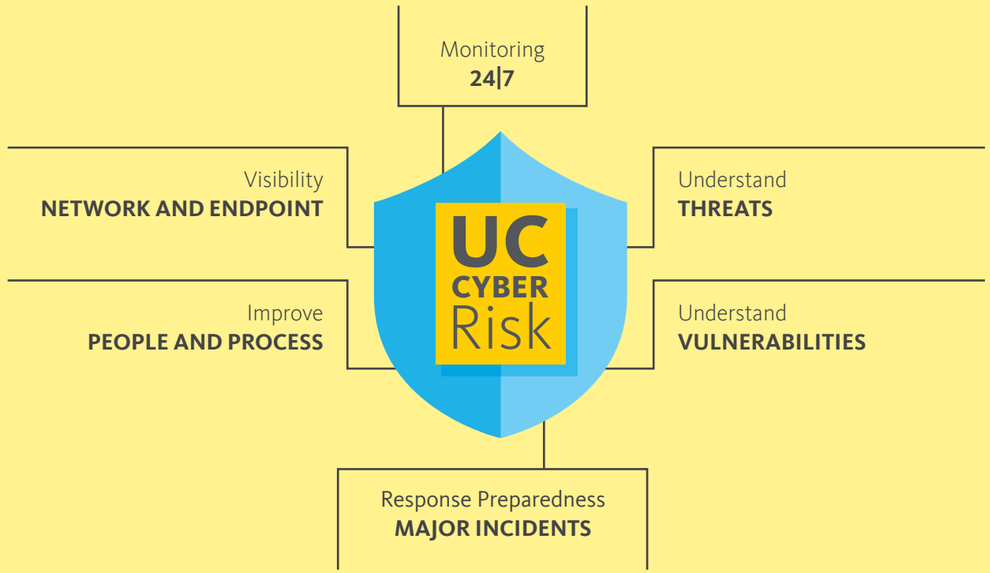
2.1%
Threat Visibility Expansion

DIGITAL THREAT MONITORING TYPES

- 80% Documents
- 10% Social Media
- 5% Network Indicators
- 2% Forums
- 2% Paste Sites
- 1% Malware Repository



PROGRAM CAPABILITIES



The High Value of Invisible Work

The challenge of successful cybersecurity programs is showing how they are valuable investments, when the best outcomes are events that never happen. But how do teams prove a negative? When we do cybersecurity well, end users often won't even know it's happening.

For example, when the COVID-19 pandemic hit, so many more people were working remotely, and cybersecurity was sometimes treated as an after-thought. But after initial efforts to ensure that people could work offsite successfully, we had to make sure work could be done securely with ease of use in mind. Working as a collaborative unit—sharing best practices and tools available to harden the system, along with stories of success and failure—made us successful. And the process for those working from home was seamless.

It's hard to measure what may have been prevented, but that doesn't mean it wasn't impactful. Through our cybersecurity work, C3 enables UC's mission to serve society as a center of higher learning, providing long-term benefits through discovering and advancing knowledge.

ADRIAN MOHUCZY-DOMINIAK,
Cyber Risk Technical Security Analyst

29 Days Saved

RESPONSE TIME SAVED
with extended detection and
Response Technologies

Source: IBM Cost of a Data Breach Report 2022, IBM Security

Best Practice Tools, Products, and Services

C3 collaborates with UC locations to enhance cybersecurity systemwide. We manage a portfolio of tools, 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.

Additionally, C3 offers consulting services that help locations determine their level of readiness. Third-party experts are available to review campus incident response programs 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:

- → **Threat Detection**
- → **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**

C3 consulting services pairs existing technologies, services, and operations with mitigation practices to manage financial impacts of data breaches:

- → **TEST** incident response process regularly to ensure cyber resilience
- → **DEPLOY** attack surface management tools to identify more threats
- → **PROVIDE** robust training on best practices for safeguarding information
- → **USE** tools to detect threats and protect endpoints, especially in remote work situations
- → **BALANCE** security and privacy when using tools and following processes to protect sensitive data

Cyber Security Summit

Our April 2022 summit was the most popular yet, with over 600 attendees. Surveyed attendees gave high marks for content, proving once again that a remote event can be focused on the human element and still offer opportunities for meaningful connection. With nine mainstage events, industry experts dissected timely issues like social engineering and ways to recognize and prevent it from happening, as well as reasons why cybersecurity can be difficult in practice. Most importantly, the summit provided tips, tricks, and advice for all levels of understanding.

Two social lounge events were offered and allowed for guided but fluid discussion about where accessibility and cybersecurity connect (or not) and how COVID-19 has changed the way we work. In addition, during a panel discussion, attendees were challenged to think about the intersection of privacy and security and how both aspects can inform and support policy in ways that will benefit those most impacted.

We're looking forward to hosting the event in person in 2023 after holding the prior five conferences virtually.

Featured Speakers:

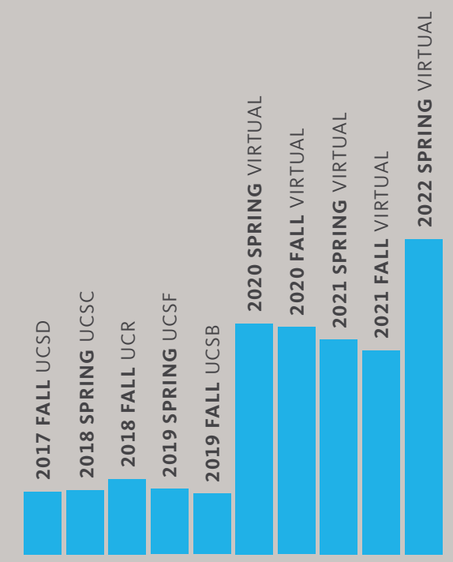
→ **JULIET OKAFOR**
JD, CEO and Founder, Revolution Cyber

→ **ED SKOUDIS**
President, SANS Technology Institute

> *Every year gets better and better. Thank you kindly for a worthwhile and productive summit that looked at security as a lifestyle and paid attention to the humans being affected. We must rethink the training needed to tackle the security threats that occur in day-to-day life, and build empathy and trust into security-related communication.*
>
> ATTENDEE
> 2022 CYBER SECURITY SUMMIT

97% Participants
WOULD RECOMMEND THE SUMMIT
TO A COLLEAGUE

Attendance trend



Award-Winning Cyber Security Summit

C3 put on the highly attended and well-received UC Cyber Security Summit. C3 was awarded the first ever Golden IT Security award in August. The summit is a collaborative effort that continues to bring together experts from across UC as well as vendors offering solutions relevant to cybersecurity at large.


UC TECH AWARDS PROGRAM
IT Security

Golden Award

Presented to the
UC Office of the President
UC Cyber Security Summit Project Team
Adrian Mohuczy-Dominiak, Jackie Porter, Wendy Rager

Van Williams
Vice President and UC Chief Information Officer
Information Technology Services
University of California Office of the President

August 16, 2022
Awarded by the UC IT
Leadership Council

Outside UC system

23% Attendees
WERE OUTSIDE OF THE UC SYSTEM
CSU, city, community, and out-of-state higher education schools

Global reach

ATTENDED BY STUDENT FROM
Adam Mickiewicz University
Poznań, Poland

Developing Good Cybersecurity Habits

Cybersecurity training updates

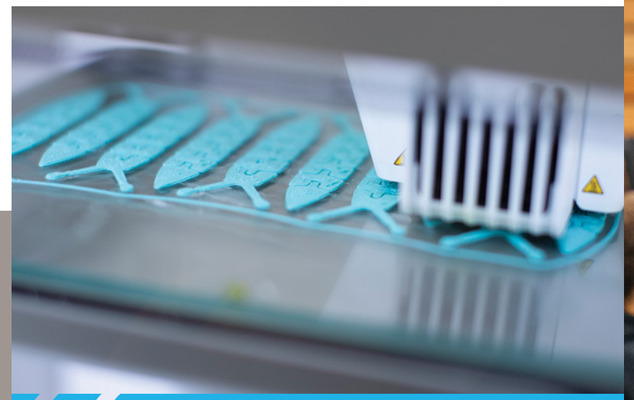
UC approached cybersecurity training by engaging a systemwide cross-section of faculty and staff to participate in designing the new mandatory Cybersecurity Awareness Training course. The result is an updated module, customized to meet UC standards. What makes this training unique is that an actual hacker delivers the training with an emphasis on issues that are relevant to campus locations and health systems. The module covers cybersecurity best practices, areas of concern to UC, and ways for faculty, staff, and students to stay cybersecure in their personal lives.

Optional training modules include topics such as:

- → Financial and identity safeguarding
- → Social media
- → Travel safety
- → Remote work habits

New role-based training for IT resources with elevated privileges

UC San Francisco introduced a role-based training for people with elevated privileges to learn about the importance of preventing credential theft and other methods of identity-based intrusion. The training first seeks to create awareness about what an individual's level of access means from a cybersecurity perspective. Building on that understanding, it then focuses on the responsibility that comes with elevated privileges and, most importantly, what choices to make or actions to take as a steward of the information they have access to. This training is especially important for high-value or high-risk targets in keeping UC secure.



With privileged access, they have more responsibility to protect sensitive information.

ESTHER SILVER,
IT Security Awareness and Training Program Manager,
University of California, San Francisco

Current & Relevant
CYBERSECURITY TRAINING
VITAL TO THE HEALTH OF
THE UNIVERSITY OF CALIFORNIA

Over 40% of most breaches in education occur due to stolen credentials.

Source: Data Breach Investigations Report 2008 – 2022, Verizon

The most common initial attack vector in 2022

19%
COMPROMISED
CREDENTIALS

Source: IBM Cost of a Data Breach Report 2022, IBM Security

If we can teach people how to safeguard their own personal information, they will develop habits that will translate to keeping workplace information safe.

CECELIA FINNEY,
Systemwide Cyber Champion Team Leader,
University of California Office of the President

Cybersecurity Awareness Month

This year's theme: Overcoming the human factor

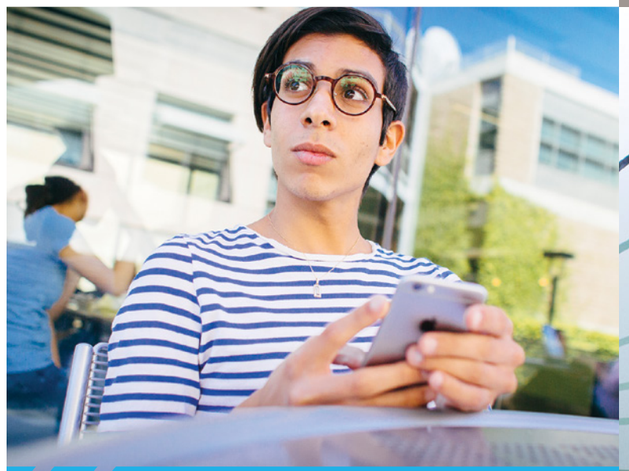
As part of ongoing efforts across campuses and health systems to educate and inform staff, students and faculty, UC's focus for Cybersecurity Awareness Month was on overcoming the human factor.

Established experts delivered on-demand and live webinars covering a wide range of topics throughout the month of October. Attendees were able to learn about cyber threats and trends, secure video conferencing, human hacking, and social engineering.

Awareness is particularly important, but a bonus result of the sessions was that they influenced students' potential careers. Some students provided feedback that they found a previously unknown interest in cybersecurity work, thanks to a session on campus with the FBI Cyber Squad.

Accessibility and security panel

A global panel of six experts convened to discuss the intersection of accessibility and security. Both topics are equally important considerations that are usually tackled as separate conversations, but bringing them together offered an opportunity to increase understanding and awareness of both sets of needs. Panelists discussed how technology can be made more accessible and secure without sacrificing important needs on either side. In fact, when accessibility and security are tackled together, outcomes are more likely to include process or practice improvements that provide benefits overall.



We have a program that benefits non-IT security people. We are doing things that are not theoretical, they're practical and they have great impact on students as well as staff and faculty.

JACKSON MUHIRWE,
CISO, University of California, Merced

82% Breaches Involved
HUMAN ELEMENT

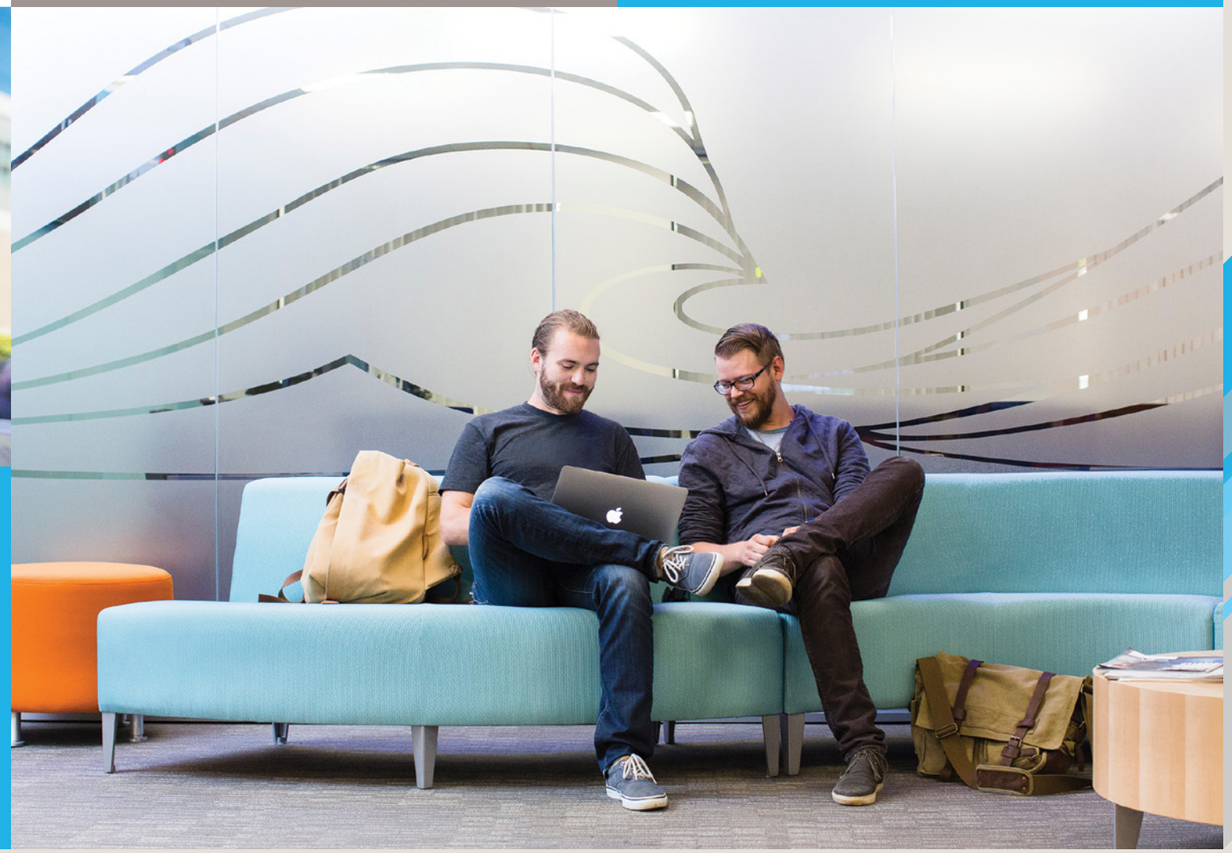
In 2022 whether they were stolen credentials, successful phishing attacks, or human error, people were at the center of many incidents and breaches.

Source: Data Breach Investigations Report 2008 – 2022, Verizon

Content from this session provided some good info to keep in mind when maintaining or creating new sites.

Thank you for holding this event. I would love to see more events related to accessibility and security in the future.

PANEL ATTENDEES



Collaborative Tabletop Exercises

When responding to a cybersecurity incident, a well-honed and understood process is key to ensuring that involved parties can act quickly and work towards fast, certain remediation. Participants worked together on coordinated tabletop exercises that mimicked real-world emergencies. Leadership was included to represent all levels of impact and response. For health systems, the Chief Medical Officer and Chief Nursing Officer provided insight to the participants to help them get a deeper understanding of how cybersecurity incidents create peripheral impacts.

In addition to health systems, campuses are adopting the tabletop exercise as a practical way to mimic high-stakes situations and proactively identify areas of improvement. A high level of involvement across stakeholders leads to feedback and problem identification that prevents additional unknown risks during future incidents. This is accomplished in part by ensuring participants have a strong understanding of their role in a cybersecurity incident and discussing and acting out steps that need to be taken in a scenario-focused environment.

It's often cited that well-coordinated communication is the reason why a critical situation was handled smoothly. Guided by this understanding, UCOP kicked off a tabletop exercise initiative in 2022 that tackles the executive communication process. Refining and improving communication drives consistency in messaging and alerts impacted populations and external audiences.

> *In addition to the genuine interest shown by all participants, I was impressed with how well the purpose of the exercise was understood and appreciated, leading to collaboration and creative thinking.*
>
> **ALLISON HENRY, CISO,**
> **University of California, Berkeley**

Breaches at Organizations

Incident Response Teams
WITH A REGULAR TESTING PLAN
$2.66M Savings

Comparison to breaches at organizations with no IR team or testing of the IR plan.

Source: IBM Cost of a Data Breach Report 2022, IBM Security

AVERAGE TOTAL COST **>$1M**
Data Breaches
REMOTE WORKING

Source: IBM Cost of a Data Breach Report 2022, IBM Security

Data Loss Prevention (DLP): Protecting Sensitive Information

Ensuring that sensitive data is protected means knowing where it is and who has access to it, and working with people to ensure access and availability don't come together to become a liability. The Data Loss Prevention (DLP) program provides an agent for laptops that identifies sensitive data and can detect when attempts are made are made to copy or move it to another location. The agent then alerts the Information Security team, and involved parties work together to identify whether the attempt was legitimate. This approach helps balance security and data availability through reliable tooling and human review.

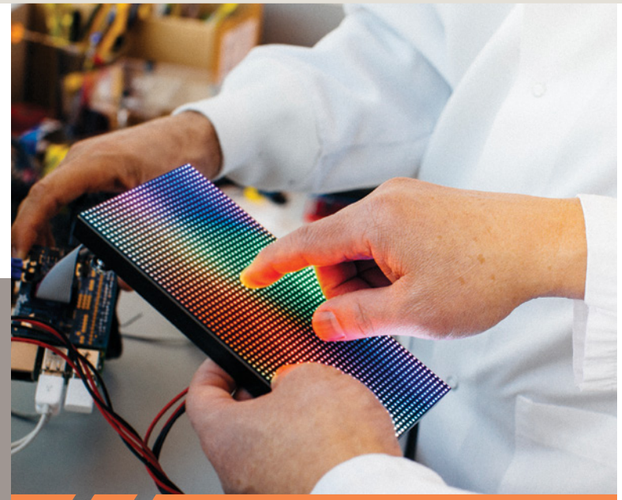
> *Our goal with DLP is to change what is necessary in our process so that we're not doing things with sensitive data that we just shouldn't.*
>
> **JOSHUA VAN HORN, Deputy CISO,**
> **University of California Office of the President**

Third Party Risk Management (TPRM): Improving the Risk Assessment Process

Ernesto Carrasco, Director of the Governance Risk & Compliance (GRC) team at UCLA, will be the first to say that collaboration is the key to improving the TPRM vendor risk assessment process. The GRC team continuously uses suggestions and requests from UCLA and vendor stakeholders to improve the process. This has most recently translated into user interface updates that consider ease of use and reduce the number of input steps required to complete a questionnaire.

AS A RESULT, the GRC team converted an all-manual process into a paper-free tool, and end users spend 33-66% less time completing vendor requests.

> *The key to the UCLA TPRM process is the ability to work collaboratively with IT Security, Accessibility, Privacy & Purchasing in real-time. In doing so, we've built a consistent, sustainable process for managing third-party risk.*
>
> **ERNESTO CARRASCO, Director, GRC**
> **UCLA**



> *It is a privilege to be a part of a system where this incredibly dedicated group of professionals from privacy, risk, law, IT, and information security come together to drive our incident responses forward through high-level thought, deep engagement, and at times, inspiring insight.*
>
> **VAN WILLIAMS, Vice President of IT and Chief Information Officer, University of California**

> *The workshop was thoughtfully prepared, especially with CISO and privacy people coming together. Being able to discuss and collaborate with colleagues across the system was so helpful.*
>
> **WORKSHOP ATTENDEE**

Incident Response and Escalation Workshop

Experts recommend not only creating but rigorously testing incident response procedures regularly to build flexibility and resilience. Fifty experts from throughout the UC system participated in a five-hour Incident Response and Escalation workshop. Bringing together a team whose collective responsibilities included cybersecurity, privacy, legal, audit, and risk, the goal was to ensure that all perspectives were represented in the process. C3 manager Wendy Rager describes the workshop as a unique opportunity for experts to collaborate and learn from each other as to what's working and what's not, and a chance to bring people together to ensure that UC responds as a team.

A POST-WORKSHOP SURVEY revealed that 93% of attendees had high degrees of satisfaction and saw value in future workshops.

Perception of Security Culture Among Organizations

85% POSITIVE
INFOSEC AND IT
Survey Respondents

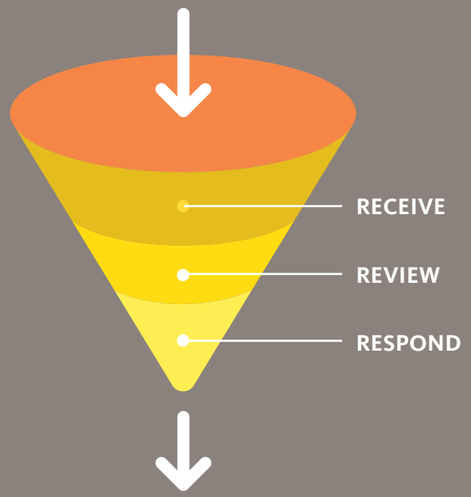
Source: Proofpoint 2022 State of the Phish Report

Protection Across the System

C3 at a Glance

Alerts Analyzed

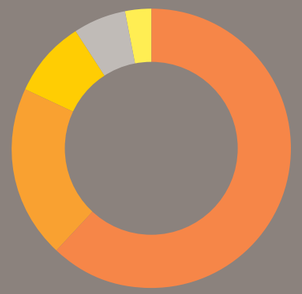
We analyze billions of alerts. This process informs our active response to minimize threats.



Types of Alerts

UC identified threat vectors in these categories to reduce impact.

- 62% Exploit-Inject Malware
- 20% Ransomware
- 9% CoinMiner
- 6% Remote Takeover
- 3% Credential Theft



C3 Achievements 2022

2X Number of New UC Health SRAs

The University of California Health System teams up with UC Health Community Connect Partners to provide medical care for patients. The partners access UC's advanced healthcare records system to make it easier to access electronic records. C3 manages Security Risk Assessments (SRAs) for the affiliates, helping to ensure HIPAA compliance and keep patient records secure.

81%

Cybersecurity Awareness training completed by faculty and staff

50%

Reduction in click rates from 2021 to 2022

Policy Corner

As a result of a collaborative, multi-year project, the University of California's systemwide policies governing security have decreased from seven to three. Additionally, the remaining policies offer people-focused improvements to make the language more accessible and increase clarity around roles and responsibilities.

2022

3 ACTIVE POLICIES

IS-3
Electronic Information Security

IS-5
Licensing and Operations, University Radio, Television and Microwave Facilities of University

IS-12
IT Recovery

***NEW AND UPDATED* RESOURCES:**

- **Gramm Leach Bliley Act Compliance Plan and Guide**
  - Account and Authorization Management Standard
- **IS-3: Electronic Information Security**
  - Standards, duties and responsibilities tool
- **IS-12: IT Recovery**
  - Role guide
- **Appendix Data Security**
  - Fillable form

***RESCINDED* POLICY:**

- **IS-11: Identity and Access Management**
  Requirements included in IS-3 and the Account and Authentication Management Standard, so the policy was no longer needed.

Information Technology Policy and Security Community of Interest

We believe that learning and information sharing are both key elements necessary for healthy cybersecurity programs. Information Technology Policy and Security Community of Interest (ITPS) is a group that encourages both, and as a result, has grown from a small group of 60 to over 600 members. Monthly meetings cover topics such as risk appetite and risk tolerance, off shoring data storage, the False Claims Act, and FTC updates. Attendees can expand their cybersecurity understanding through case studies, threat briefings, and training.

ITPS is open to anyone at UC with a role or interest in IT policy or cybersecurity.

50% ITPS Membership Growth 2021-2022

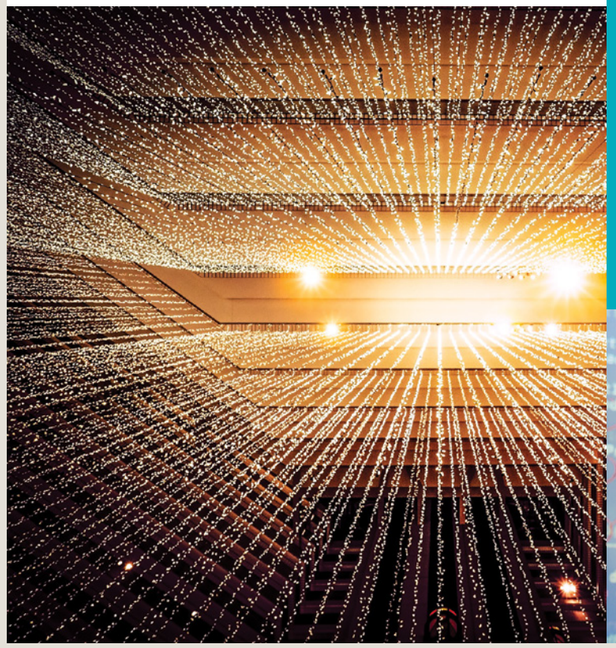
UC Davis Establishes Guardrails for Working with Sensitive Data

As UC Davis Professor Matt Bishop explains, synthetic statistics and data don't always meet organizational information needs. This is especially true when researching types and areas of internet behavior that allow for tracking potential cybersecurity threats. However, a significant concern when working with real data is that it will be used for non-research reasons, and this is an issue that can't be solved in a bubble.

In pursuit of an answer that considers the necessary balance between security and privacy, UC Davis faculty, CIO, and CISO partnered to create a guardrail agreement to use the real data in question. It covers several important areas of concern, such as how long the data can be used, what permission levels are required for access, and acceptable use definitions.

With clear guidelines established, an invested group of faculty, staff, and students say this agreement has opened the door to more meaningful research. Bishop will be working with students and testing the theory that anonymized data is as every bit as good as non-anonymized data. This real data can also be used to build statistical internet behavioral models to identify roles, create profiles, and then search for unusual behavior patterns based on those roles.

In 2023, find out if the theory that anonymized data is as good as data that hasn't been scrubbed holds true and what the results mean for cybersecurity work to come.



This is an incredible example of working together to make improvements that serve the greater good without sacrificing important needs in the realm of privacy, legal, and compliance.

MATT BISHOP, Professor, Department of Computer Science, UC Davis, Chair of University Committee on Academic Computing and Communications (UCACC)

Hands On: The Master of Information and Cybersecurity from UC Berkeley

The UC Berkeley School of Information's Master of Information and Cybersecurity (MICS) program offers students an opportunity to gain hands-on experience with penetration testing of real campus applications. This occurs under the guidance of an expert instructor and the Berkeley Information Security Office. Like all courses in the 20-month part-time MICS degree program, the Web Application Security Assessment class meets online in the evenings for the convenience of students across the country and worldwide. Most are full-time working professionals, and everyone is working toward a degree that develops both practical and theoretical understanding of the technical, business, political, and legal areas of cybersecurity.

This class's hands-on approach benefits not only students, but also the campus application owners and developers, as they receive a semester-end report detailing their application vulnerabilities. Identifying potential vulnerabilities before they can be exploited helps to reduce the risk of sensitive data exposure and potential losses. In addition, an equivalent report from external consultants would be cost-prohibitive.

This practicum class is an advanced elective in the MICS leadership-focused interdisciplinary curriculum, where graduates finish with comprehensive skills in areas such as secure coding, operating system security, privacy engineering, and much more.

A Leadership-Focused Curriculum

Secure Coding

Government and National Security

Network and Web Security

Usable Privacy and Security

Cryptography

Operating System Security

Security in Context: Legal, Behavioral, and Ethical Issues

Privacy Engineering

Cyber Risk

Working with the MICS students was a great experience. They found a handful of things that we missed in code reviews and a few things that we just plain missed.

STEVEN HANSEN, Application Developer, University of California, Berkeley

This course was my first real deep dive into Web Application security testing. The real hands-on experience [...] really helped grow my understanding of Web Application security. I have since used the practices I learned in this course to train others in my professional circle, and I've used the principles taught to argue for increased testing coverage of systems that I work with. All said, this is one of the most immediately applicable and useful courses I have taken in the MICS program.

JACOB GLAD, Student University of California, Berkeley

The Landscape

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 2022 landscape. At UC, we're bringing people together across campuses and health systems to collaborate and learn how to develop a systemwide security mindset.

Risks at a Glance:

- → **16.6%** more time to contain stolen or compromised credentials
- → **19%** of breaches are linked to stolen credentials
- → **80%** organizations without Zero Trust
- → **82%** of breaches are driven by the human element
- → **$4.35M** average cost of a data breach in 2022
- → **$4.91M** average cost when phishing was the initial attack vector

Benefits at a Glance:

- → Organizations save money and time with AI, reliable incident response, and participating in threat sharing
- → **3.5%** average remediation time
- → **10%** faster response time with XDR
- → **$2.66M** incident response team and testing
- → **$3.05M** fully deployed AI and automation
- → **29 Days** saved by extended detection and response

Changes from 2021 to 2022:

- → **2.6%** average increased cost of each breach
- → **3.2%** increase in ransomware breaches
- → **10.7%** decrease in lost business costs
- → **21%** increase in the use of security AI and automation
- → **32.6%** decrease in cost with security AI
- → **60%** of organizations increased prices of products and services

Sources: IBM Cost of a Data Breach Report 2022, IBM Security; Data Breach Investigations Report 2008 – 2022, 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