UC Cyber Risk Program
2024 Report

UNIVERSITY OF CALIFORNIA

Industry Predictions for the Future of Cybersecurity

THROUGH **2025**

securing generative AI will drive

A MORE THAN 15% INCREMENTAL SPEND

on cybersecurity resources

BY **2027**

50% of large enterprise CISOs will adopt

HUMAN-CENTRIC SECURITY BEHAVIOR

and design practices to minimize human risk and maximize control adoption

BY **2028**

enterprise spend dedicated to battling malinformation, a new threat vector,

WILL SURPASS $30 BILLION,

cannibalizing 10% of marketing and cybersecurity budgets

SOURCES:

Gartner Research Predicts 2024: *AI & Cybersecurity — Turning Disruption Into an Opportunity.*
Gartner (2024, February 22). *Gartner Identifies the Top Cybersecurity Trends for 2024* [Press release].
McCartney, Ava. (2023, December 4). *Gartner's Top Strategic Predictions for 2024 and Beyond.*

> “ *This year, we've seen governance and compliance converge, with new standards and external factors shaping our tools and practices. These overlapping requirements highlight key issues we must address, especially where compliance intersects with systemwide needs. We're focused on building a roadmap to strengthen our systemwide approach.*
>
> **VAN WILLIAMS**, Vice President of IT and Chief Information Officer, University of California

Welcome

As we reflect on another year of progress, we're proud to highlight how far the Cyber-risk Coordination Center (C3) group has come in making the University of California more cyber secure. Over the last decade, C3 has been dedicated to safeguarding UC's digital landscape. To commemorate this journey, we've created a timeline capturing some of the most significant events that have shaped our cybersecurity efforts.

With strong executive-level support, we've moved beyond creating and executing cybersecurity awareness programs to making these efforts even more efficient by streamlining operations and maximizing our cybersecurity investments. Some of our ongoing initiatives—such as the IT Policy and Security (ITPS) Community, Cybersecurity Awareness Month, Cyber Security Summit, and UC Tech Academy programs—show lasting impact, helping us foster a more secure environment systemwide.

This report also features stories highlighting innovative approaches and improvements to cybersecurity. From defining a vision centered on digital risk to combating credential phishing to reducing attack surfaces, these stories showcase the evolving landscape and UC's continued commitment to cybersecurity excellence.

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

SYMBOL KEY FOR THIS REPORT:
⊕ Read more on our website
⊛ Read more in this report

Cyber Risk Management at UC

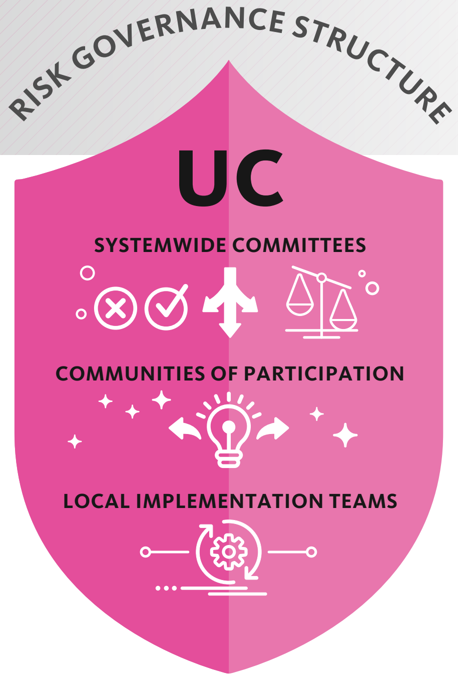
Our Approach to Cybersecurity Is Structured Around Five Pillars

1. **GOVERNANCE** Enhancing governance structures helps us coordinate cybersecurity efforts.
2. **MANAGEMENT** Strengthening risk management ensures consistent efforts across UC.
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 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. These groups serve the campuses, health centers and laboratories.

1. **SYSTEMWIDE COMMITTEES**
   - Cyber Risk Governance Committee
   - IT Leadership Council
   - UC Information Security Council ➔ **Page 5**
   - Ethics, Compliance, and Audit Services
   - University Committee on Academic Computing and Communications
2. **COMMUNITIES OF PARTICIPATION**
   - UC Security Incident Response Coordination
   - IT Policy and Security (ITPS)
3. **LOCAL IMPLEMENTATION TEAMS**
   - Leveraging Scale for Value
   - Center for Data Driven Insights and Innovations


RISK GOVERNANCE STRUCTURE
UC
SYSTEMWIDE COMMITTEES
COMMUNITIES OF PARTICIPATION
LOCAL IMPLEMENTATION TEAMS

> *Since joining this community, I feel more plugged into the IT security and policy and privacy initiatives going on at UC... Excellent way of sharing across UC communities... Interesting, relevant, and helps bring contextual awareness!... Always helpful and practical information.*
>
> **ITPS MEMBER INSIGHT**

COLLABORATIVE CYBERSECURITY INITIATIVES

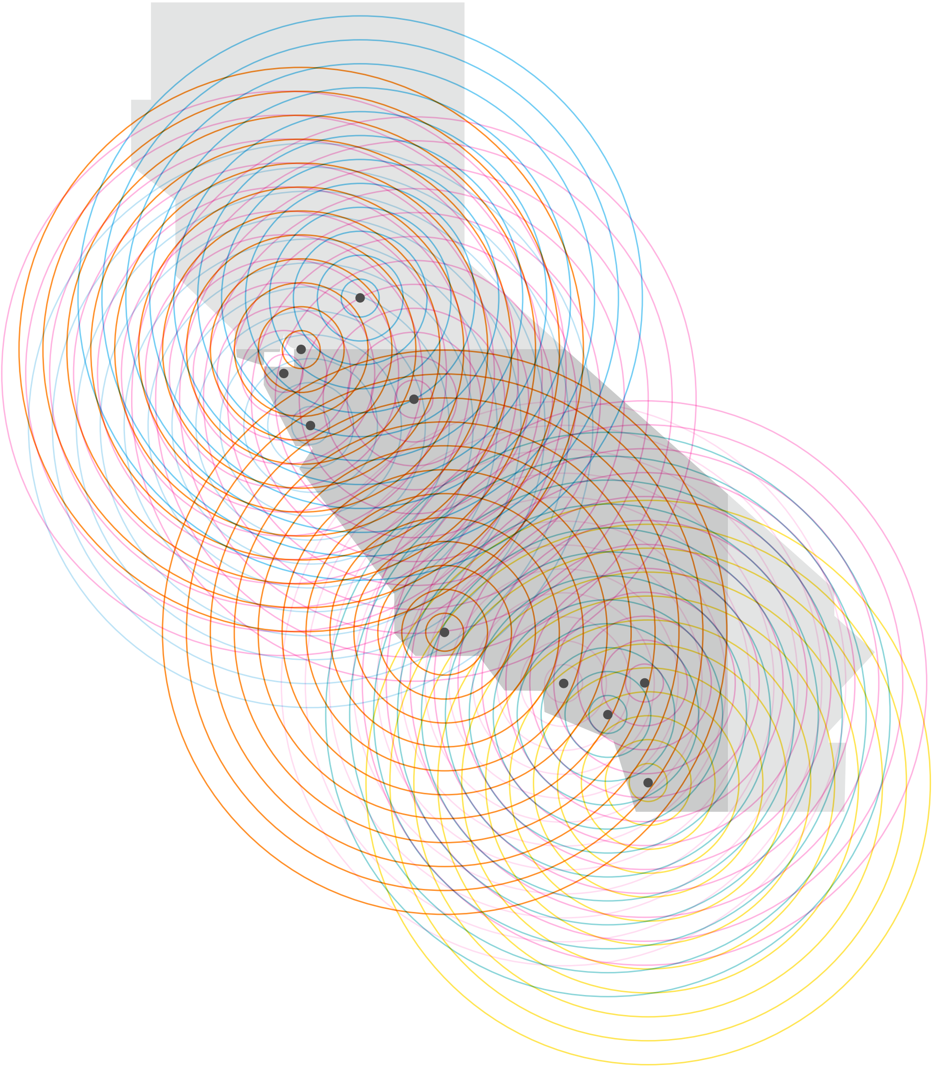
The Role of the Information Security Council

The UC Information Security Council (ISC) is one of the systemwide committees and is composed of Chief Information Security Officers (CISOs) from all UC locations, the executive ISC, and ex-officio members. Chartered by the UC Chief Information Officer (CIO) Council, the primary responsibility of the ISC is to serve as a consulting and advisory body on cybersecurity initiatives to the Systemwide CISO, UC CIO Council, Cyber-Risk Governance Committee (CRGC), Council of Chancellors, President of the UC System, and other UC Leadership. The work of ISC supports UC's mission and drives collaborative cybersecurity initiatives that yield mutual benefits for UC locations and the UC system as a whole.

⊕ UC Information Security Council
⊕ UC Chief Information Officer Council

ISC MISSION

To identify, prioritize, sponsor, provide expert advice, and implement programs to enhance cyber resilience of individual locations, the entire UC system, and the greater cybersecurity community.



The C3 Journey

Milestones of Innovation and Impact

The C3 timeline highlights significant milestones and pivotal events that have shaped our journey and impact over the years. Each entry reflects our commitment to innovation, collaboration, and growth.

MILESTONE ABBREVIATIONS

C3	Cyber-risk Coordination Center
CRGC	Cyber-Risk Governance Committee
CREs	Cyber-Risk Responsible Executives
TDI	Threat Detection and Identification
NIST	National Institute of Standards and Technology
SRA	Security Risk Assessment
SIREN	Systemwide Incident Escalation Report and Notification
IRPS	Incident Response and Prevention Services
SLA	Service Level Agreement
CTIAS	Cyber Threat Intelligence Analytic Services
AIM	Applied Intelligence Mentorship
CTI	Cyber Threat Intelligence

2015

C3 was created to unify UC's cybersecurity efforts, supporting faster response to threats, systemwide governance, and heightened cybersecurity awareness systemwide.

The CRGC was established with CREs to oversee investment strategies and coordinate systemwide cybersecurity efforts.

2016

The inaugural UC Cyber Security Summit was held at UC Irvine as a systemwide day of presentations and networking.

The Systemwide Security Awareness Team was established (and later renamed Cyber Champions) to collaborate on creating security awareness resources.

2017

The TDI program went live at two UC locations with a collection of cybersecurity tools, services, and expertise.

C3 led a Current State Assessment according to NIST's Cybersecurity Framework to capture the current state of cybersecurity efforts.

2018

An SRA process was standardized at each UC Health location, supporting consistent risk management in their partnerships.

The TDI Program was implemented systemwide, equipping UC with consistent real-time threat detection and response tools.

2019

The SIREN tool was launched to standardize systemwide incident response and improve coordination for significant cybersecurity events.

The IS-3 Electronic Information Security Policy was created to provide a systemwide framework for reducing and managing cyber risk.

2020

UC Cyber Security Summit went virtual due to the COVID-19 pandemic.

UC surpassed 500K completed cybersecurity trainings.

2021

IRPS implemented a 2-hour SLA for critical incidents that provided a faster response time for containment and recovery from cyber breaches.

CTIAS program was implemented to enhance UC's ability to detect and respond to emerging cyber threats.

2022

Incident Response and Escalation Workshop was held to unite experts systemwide from cyber, privacy, legal, audit, and risk.

C3 was awarded the first-ever peer-voted Golden IT Security award for the UC Cyber Security Summit.

2023

UC Tech Academy: AIM was launched to build and enhance systemwide CTI expertise.

UC Tech Academy: Cyber Leadership Program was launched to equip UC leaders with collaborative ways to manage digital risk.

2024

A new, centralized Cyber Risk Assessment Unit was created to strengthen third-party supplier and UC location cyber risk assessments.

Human Risk Training delivered to the systemwide UC Cyber Champions Group.

Cyber-risk Coordination Center Tools and Services

The Cyber-risk Coordination Center (C3) provides comprehensive services and tools to enhance cybersecurity across the University of California system. Collaborating with UC locations, C3 manages a robust portfolio of best-practice tools, products, and services designed to help campuses, health centers, and labs effectively manage cybersecurity, reduce risks, and respond to threats. Through strategic coordination and expert guidance, C3 equips UC locations to stay ahead of the latest cybersecurity threats, safeguarding the institution’s critical missions of education, research, healthcare, and public service. ⊕ **C3 Services**

C3 ACHIEVEMENTS 2024

90%
of faculty and staff completed cybersecurity awareness training

708
Members of the IT Policy and Security (ITPS) Community

C3 TOOLS AND SERVICES

- CONSULTING SERVICES
- POLICIES, STANDARDS & GUIDELINES
- THREAT INTELLIGENCE
- INCIDENT RESPONSE COORDINATION
- TRAINING & AWARENESS
- THREAT DETECTION & IDENTIFICATION
- SECURITY RISK ASSESSMENTS

C3 at a Glance

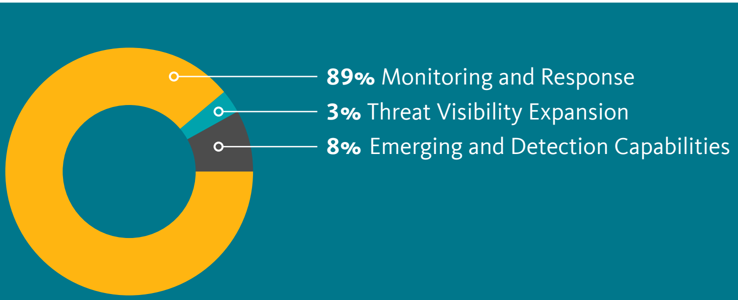
The Threat Detection and Identification (TDI) program is a collection of cybersecurity tools, services, and expertise that helps UC identify cybersecurity potential threats, provide network and endpoint visibility, and enable a better understanding of threats and vulnerabilities. TDI harnesses UC and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

Digital Threat Monitoring (DTM)

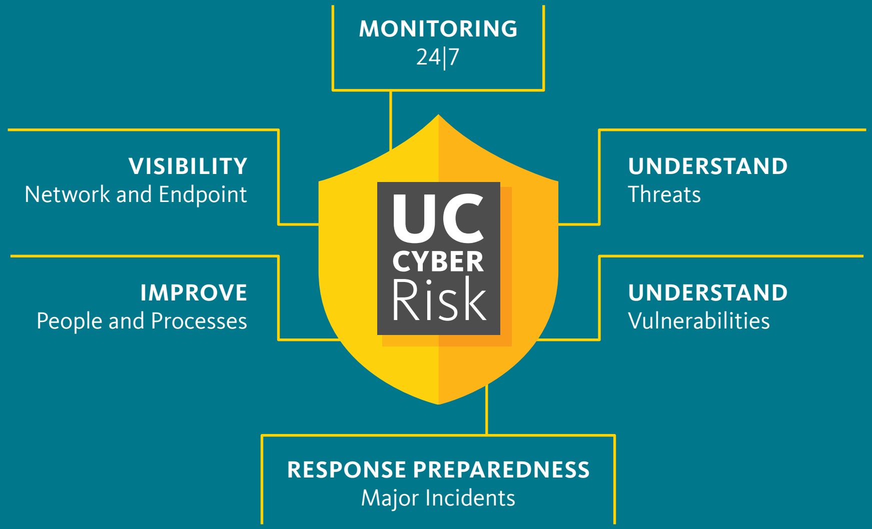
DTM allows us to analyze high-risk attacks from the open, deep, and dark web. These threats originate from various sources, and our tools help us focus on the most significant ones. In 2024, the top alert types were domain discovery, compromised credentials, and messages.

Threat Detection and Identification (TDI) Investment

We invested in the following areas to support our TDI program.

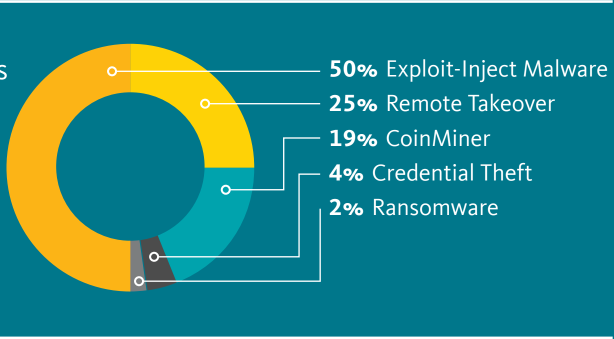


Program Capabilities



Alerts Analyzed

C3 identified threat vectors in these categories to reduce impact.



UC Health Affiliate Security Risk Assessments

The University of California Health System partners with UC Health Community Affiliates, granting them access to UC's advanced healthcare records system. C3 manages Security Risk Assessments for these affiliates, ensuring HIPAA compliance and safeguarding patient records. In 2024, more than 50 Security Risk Assessments were performed.

DRIVING INNOVATION

Service Enhancements

As cybersecurity threats grow more complex, service and tool capabilities are continuously enhanced to provide the most effective solutions. The service initiatives outlined in this story span various areas of cybersecurity, reflecting ongoing efforts to strengthen detection and response while also expanding targeted learning opportunities. These initiatives, some of which fall under the Threat Detection and Identification (TDI) program, showcase the advancements to improve UC's overall security posture.

Simulated Real-World Cyberattack

UC San Diego piloted a new, immersive training experience that allowed participants to respond to realistic cyberattack scenarios in a controlled, consequence-free environment using industry-standard tools. ⊕ **Page 12**

UC Tech Academy

This year, UC Tech Academy expanded its Digital Risk Leadership and Applied Intelligence Mentorship programs, adding more education, collaboration, and networking opportunities to support leaders in navigating emerging digital risks. ⊕ **UC Tech Academy initiatives**

Shift to Human-Risk Management

The shift in industry focus from gamified training to human-risk management marks a new approach to security awareness. This method emphasizes behavioral change and proactive risk management, signaling a meaningful evolution in training priorities. ⊕ **Page 11**

> *The Digital Risk Leadership course content, variety of speakers, and interactive discussions were valuable. The program also emphasized that effective risk management is a shared responsibility, requiring partnership across all levels. I highly recommend it to professionals looking to deepen their understanding of digital risk management.*
>
> **ROSHNI PRATAP**, Director, Strategic Sourcing, Office of the President

TDI Program Enhancements

The TDI program continues to evolve as we explore new technologies that offer enhanced features and functionalities. These advancements are designed to integrate seamlessly into UC's infrastructure, providing more robust and adaptable solutions for managing technical risks.

AI and Cybersecurity at UC

As AI technology advances, UC leads discussions and initiatives through collaborative efforts, working groups, and committees. These initiatives focus on understanding and integrating AI's role in enhancing cybersecurity and education. ⊕ **Page 16**

Advancing Cybersecurity Metrics

We evaluate systemwide cyber metrics to gain insights into digital risk management across UC. By analyzing metrics such as percentage of endpoints with Endpoint Detection and Response (EDR), percentage of high-risk systems monitored by security, and percentage of vendors without a Vendor Risk Assessment (VRA), we're better equipped to understand the evolving threat landscape. This helps us prioritize risks and improve decision-making to protect institutional information and IT resources.

Managing Human Risk Training Brings UC's Systemwide Cyber Champions Group Together

When Cecelia Finney, Manager of Systemwide Cybersecurity Awareness, Training, and Human Risk Strategy at the Office of the President, took a Managing Human Risk course in August 2023, she saw an opportunity to bring the training to UC's Cyber Champions Group. This group of security experts, including analysts, compliance professionals, engineers, developers, and CISOs, is dedicated to strengthening UC's culture of cybersecurity. Finney recognized that the UC Human Risk Management (HRM) program could benefit from this knowledge. The training, held at UCLA on August 13-15, 2024, brought together over 20 participants, marking the first in-person meeting in nine years.

Two Primary Objectives of Training

1. EMPOWER the team with a structured approach to managing human risks at UC, focusing on practical priorities rather than theoretical concerns.
2. ELEVATE the maturity of UC's cyber awareness programs by effectively managing behaviors associated with these risks.

> *The Managing Human Risk course was outstanding! The course content was insightful, relevant, and contained valuable information. I especially enjoyed the lab sessions that allowed me to collaborate with my UC peers. I gained fresh ideas on how to positively impact our security awareness program at UC Santa Barbara.*
>
> **ROGER PADILLA, JR.**, CISSP, Senior Systems Engineer, Unit Information Security Lead, UC Santa Barbara

50% of Large Enterprise CISOs will adopt human-centric security behavior and design practices to minimize human risk and maximize control adoption BY **2027**

WHAT IS HUMAN RISK MANAGEMENT?

Cyber threat actors have changed their attack methods, they no longer target technology but people. Human Risk Management (HRM) is the structured approach in how organizations secure people, addressing for most organizations what is now their greatest vulnerability—their workforce.

SOURCES: Gartner (2024, February 22). *Gartner Identifies the Top Cybersecurity Trends for 2024* [Press release]; The SANS Institute

UC San Diego Pilots a Simulated Real-World Cyberattack Training Program

Teams deepened their understanding of each other's roles and work processes during the training.

> *Let's do this!... Document everything!... What's our next step?... I wish I would've followed up on my hunch...*
>
> **ATTENDEEE INSIGHTS**

The Threat Detection & Response (TDR) team at UC San Diego piloted the first experience-based educational cyberattack training program provided by a third-party partner on July 29-31, 2024. The program provided a realistic, consequence-free environment designed to simulate real-world cyberattack scenarios, enabling participants to practice incident response procedures using industry-standard tools and techniques. Participants included members of the TDR team, security, the Windows Active Directory (AD) team, and the Identity & Access Management team.

During the training, facilitators set up virtual corporate networks, replicating a real-world environment, and performed advanced persistent threat (APT)-level attacks with dynamic engagement rules. The program allowed organic changes to the scenarios and enabled attendees to hone their skills against attacks.

Cheo Codda, Threat Detection & Response Manager at UC San Diego, noted that one of the training's benefits was improved collaboration among the different security teams. While the teams work under the same umbrella of Security or the Office of Information Assurance (OIA), they usually engage with each other in more proactive endeavors. During the training, the teams worked together, improving their understanding of each other's processes and fostering camaraderie.

COLLABORATION: A KEY TAKEAWAY FROM THE TRAINING

The AD team usually doesn't see how the TDR team handles security incidents, so this experience gave both teams valuable insight into how others work. The insight will help the AD teams anticipate the TDR team's needs, improving response time. In addition, the AD team's Windows expertise helped the TDR team identify unusual activities and interpret suspicious actions, which will lead to faster resolutions in the future.

CONVERSATIONS TO ACTION

Strengthening Cybersecurity at UC

In today's rapidly evolving threat landscape, conferences and other gatherings play a critical role in strengthening a university's cybersecurity defenses. These events provide valuable opportunities for cybersecurity professionals to stay ahead of emerging threats, share best practices, and gain insights from industry experts and peer institutions.

In addition, gatherings yield significant tangible outcomes. At UC, cohort-led discussions, expert-led sessions, and UC-specific conferences result in actionable insights, such as implementing best practices and updating training programs. These outcomes go beyond mere conversation, driving the adoption of new strategies that mitigate risks and improve UC's ability to respond to cyber threats. Events aren't just a platform for exchanging ideas—they're catalysts for implementing meaningful changes that strengthen cybersecurity systemwide.

Demetrios (Laz) Lazarikos, career CISO, AI researcher, and business advisor, presents at the 2024 UC Cyber Security Summit.

SOME OF THE MANY GATHERINGS THIS YEAR INCLUDED

- UC Cyber Security Summit ➔ Page 14
- AI Academic Congress ➔ Page 16
- 2024 UC Tech Annual Conference
  - UC Berkeley's IS-3 Risk Assessment Journey ➔ Page 25
  - UC Berkeley's Running a Successful Tabletop Exercise: Demystifying the Process and Offering Practical Tips for All Levels
  - Journey to Develop an IT Accessibility Program for UC Merced and UC Santa Cruz
  - UC San Francisco: Unraveling Potentials and Pitfalls of AI, One Experiment at a Time
- 2024 Ethics, Compliance and Audit Symposium
  - Fireside Chat with US Attorney: Collaboration with DOJ in Safeguarding the UC
  - UC Irvine's Software/IT Services Vendor Risk Reviews: Lessons Learned and Future Opportunities
  - UC Berkeley and UC Office of the President: Cyber Risk Ownership and Acceptance, UC Best Practices & Example Use Cases

Fostering Community Through Events

15th Cyber Security Summit: Protecting Today, Innovating Tomorrow

On October 9, 2024, over 200 professionals gathered at UC Irvine for the 15th Cyber Security Summit. Through presentations and collaborative discussions, this event furthers our collective mission of research, education, and public service. Presenters included experts from various fields, such as customer service, data breach resolution, and systems engineering. Presentations covered resource constraints, alert fatigue, sensitive data protection, the cyberattack industry, and responsible AI and machine learning. The event was a valuable opportunity to reconnect, build new relationships, and inspire cybersecurity advancements. ⊕ **15th Cyber Security Summit**

ATTENDEE DATA

50% First time **15%** 4+ Summits

SATISFACTION RESULTS

95% of participants were very satisfied or satisfied with the overall event

95% of participants were extremely likely or likely to attend and recommend our summits to a colleague

THE 15TH
CYBER SECURITY SUMMIT
Protecting Today, Innovating Tomorrow

UNIVERSITY OF CALIFORNIA

OCTOBER 9, 2024
UC IRVINE, UCI STUDENT CENTER & EVENT SERVICES

Cybersecurity Awareness Month: Protect Your Digital Life – Be CyberSafe

October marks cybersecurity awareness month, a time dedicated to raising awareness about the growing importance of protecting personal and organizational digital assets. This year's campaign, Protecting Our Digital Lives, included discussions and themes around the evolving role and presence of AI in our lives. While AI can keep us safe online, it's important to remember that cybercriminals can exploit it for malicious purposes.

Through webinars, expert discussions, and interactive sessions, participants learned how to protect their personal information and professional data, while understanding the evolving threats posed by advanced technologies. The campaign underscored the importance of staying informed and being proactive in a rapidly changing digital landscape.

⊕ **Cybersecurity Awareness Month**

CYBERSECURITY AWARENESS MONTH EVENTS INCLUDED

- **So You Think You Know IT Security -** a knowledge contest where attendees answer a variety of questions related to keeping UC's data and computing devices safe and secure.
- **You Didn't See It Coming: Cyber Risk in Higher Education -** a presentation by former UC Santa Barbara CISO, Matthew Hall, on the rapidly evolving landscape of cyber threats facing universities and colleges.
- **Hot Tips for Being Cyber Safe in Today's Threat Environment -** a presentation by Morgan Adamski, Executive Director of U.S. Cyber Command, about the latest cyber threats to national security and our roles in protecting ourselves and the United States.
- **Privacy, AI, and Cyberlaw 101 -** a discussion on how we approach data protection and governance, given the increased convergence of privacy, cybersecurity, and artificial intelligence.

Unique Semi-Truck Tour at UC Irvine Equips Students for Success in Cybersecurity

In celebration of Cybersecurity Awareness Month and in conjunction with the UC Cyber Security Summit held this year at UC Irvine, members of the Cyber@UCI Club toured a high-tech cybersecurity command center housed in a semi-truck provided by one of our partners. The hands-on experience exposed students to advanced cybersecurity technologies and real-world scenarios.

The student-led Cyber@UCI Club supports career readiness in cybersecurity by offering skill-building opportunities, peer collaboration, and professional engagement. During the tour led by industry experts, students explored both virtual and physical displays of top threat detection systems, firewalls, and security platforms. The experts also shared insights into practical defense tools, emerging trends, and career pathways.

This event showcased the value of partnerships between academia and industry in preparing the next generation of cybersecurity professionals.

“Our takeaway is that this event made it clear that students are pretty eager to learn more about what industry is like and how to best prep for it beyond coursework, so we will be aiming to help facilitate this more,” said Steven Ngo, a representative of Cyber@UCI Club.

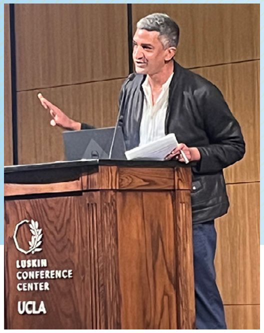
Cyber@UCI Club members inside the semi-truck.

> *Helping the new generation understand key cybersecurity concepts and the different aspects of this field is incredibly rewarding. We didn’t have these opportunities growing up, so seeing the students engage so deeply is exciting.*
>
> **TONY ALAFAR,** Software Engineer and Tour Leader

> *Having professionals care about our education and success is encouraging. It reinforces my belief that cybersecurity is the future and that we’re stepping into an important, growing field.*
>
> **CARA FAILER**, Graduating Fourth-Year Software Engineering Major and Cyber@UCI Club Member

2024 UC ACADEMIC CONGRESS

AI Sparks Insightful Dialogue



As AI technology continues to advance rapidly, UC is at the forefront, driving discussions and initiatives through various working groups, committees, and collaborative efforts focused on the role AI plays in education.

In February 2024, a diverse assembly of experts from across UC's 10 campuses, three national labs, and six academic health centers convened to explore the university's role in shaping AI for the public good. UC's Provost, Katherine S. Newman, and UC Chief Information Officer, Van Williams, hosted "What the Future Holds: A UC Congress on the Impact and Promise of Artificial Intelligence." UC leaders in attendance included President Michael V. Drake and former university president Janet Napolitano. The event featured keynote speakers, panelists, and others who presented research on AI's effect on labor markets and the broader economy, the role of UC in protecting data privacy, algorithmic bias, and how to best prepare students for the workforce given these important new developments.

SOURCE: https://uctechnews.ucop.edu/2024-uc-academic-congress-on-artificial-intelligence-ai/

CONFERENCE TAKEAWAYS

- **UC has been in the vanguard of AI research and application for the last 30 years**—since UC Berkeley professors Stuart Russell and Peter Norvig wrote the fundamental textbook for AI in 1995.
- **The University has demonstrated its leadership in addressing the governance of AI within the university context,** starting with the UC Presidential Working Group on Responsible AI, launched by President Drake in fall 2020.
- **While AI holds promise** for enhancing productivity, accuracy, and efficiency, addressing key challenges such as excessive automation and information monopolization and manipulation is crucial to ensure that AI benefits society as a whole.
- **By fostering a nuanced understanding of AI's scope,** policymakers, businesses, academia, and individuals can navigate the future of work, education, research, and patient care in the era of AI more effectively.
- **Participants welcome the opportunity to continue the conversation.** Next, the UC AI Council aims to establish a baseline set of principles for AI governance, coordinate with various stakeholders, harmonize definitions across campuses, and provide a central resource for AI-related information.

⊕ **UC AI Council**
⊕ **Presidential Working Group on AI**
⊕ **AI at UC**

UC SAN DIEGO HEALTH PHI CLEANUP

Combating Credential Phishing One Email at a Time

In early 2023, UC San Diego Health launched a first-of-its-kind risk mitigation effort to address phishing-related data breaches.

GOAL

Recognizing that email systems have become an archive of sensitive data over time, UC San Diego Health aimed to identify emails containing large amounts of potentially sensitive data.

APPROACH

1. Significantly reduce the impact of data loss by scanning emails for potentially sensitive data, such as Protected Health Information (PHI), Personally Identifiable Information (PII), credit card numbers, and more.

2. Delete this data from user email accounts using a web application and established processes, and communicate project information to stakeholders.

IMPLEMENTATION

1. Scans were conducted on all email accounts within the email tenant using various vendor partners' tools.

2. UCSD Web Services built a tool to consolidate scanned data, show individuals their scanned results, and support a deletion exception process.

3. Continuous communication was maintained with users and leadership committees through emails and presentations to ensure stakeholders were informed about the project's progress and required actions.

OUTCOMES

8+ months to complete scanning

20 virtual servers ran the scanning application

6,500+ users had at least one email with more than 200 records of sensitive data

40,500+ email accounts scanned

154,000+ individual emails scanned

29 Million total PHI/PII data elements moved to a secure location

1.25 Billion total PHI/PII data elements removed or deleted

1.5 Billion individual pieces of sensitive data flagged for review

Compromised Credentials and Phishing were responsible for 16% and 15% of breaches, respectively.

SOURCE: IBM Cost of a Data Breach Report 2024, IBM Security

UCLA HEALTH REDUCED ATTACK SURFACES

It Took a Village with Regular Communication

Checking off a completed project is a great feeling, but nothing compares to the satisfaction of happy customers—especially when they take the time to provide glowing reviews! That's exactly what happened with UCLA Health's initiative to reduce cyberattack surfaces by blocking non-standard remote access tools and encrypted tunnel applications to medical devices.

Given the complex environment and many barriers, the best approach for UCLA Health was to address applications with firewalls. This approach aimed to reduce exposure to cyber threats and increase efficiency.

It was not an easy feat. Faced with a diverse user base, including IT, clinical staff, faculty, and researchers, the initiative's team knew it would be a tough cultural shift. The team focused on two core competencies: understanding users' needs and communication.

BENEFITS

- Over 175 unauthorized remote access applications were blocked
- Huge bandwidth savings on firewalls

The Core Team:

- Documented use cases and identified key partners from several functional areas who interfaced with end users. They mapped out a phased approach, starting with simple fixes and progressing to specialized applications. When tunnel apps were discovered, the team expanded the scope to tackle that as well. The team learned and shared their successes with each project phase.
- Kept end users at the forefront of the entire project, sending regular communication several times before they took any action. The communications explained what was happening, when, and why these measures were necessary. They also explained how bad actors have become more tech-savvy and included educational resources such as a link to their policy and examples of recent cybersecurity breaches.
- Covered all aspects of the project and worked together in partnership with firewall and communication teams and business relationship managers. Not only was the project completed on time, but it also earned praise from users, including thank-you notes from physicians and others for safeguarding their data.

PROJECT SPONSORS
PROJECT TEAM
ADVISORY AND GOVERNANCE COMMITTEES
SUPPORTING IT ROLES

> “*Thank you for making our clinical area safe and secure. We didn't know (a remote access tool) was installed on my laptop.*
>
> **UCLA PHYSICIAN**

> “*Thank you for helping me easily onboard an IT-supported solution.*
>
> **UCLA RESEARCH STUDENT**

> “*Thank you for the massive communication to avoid any surprises.*
>
> **UCLA DEPARTMENT HEAD**

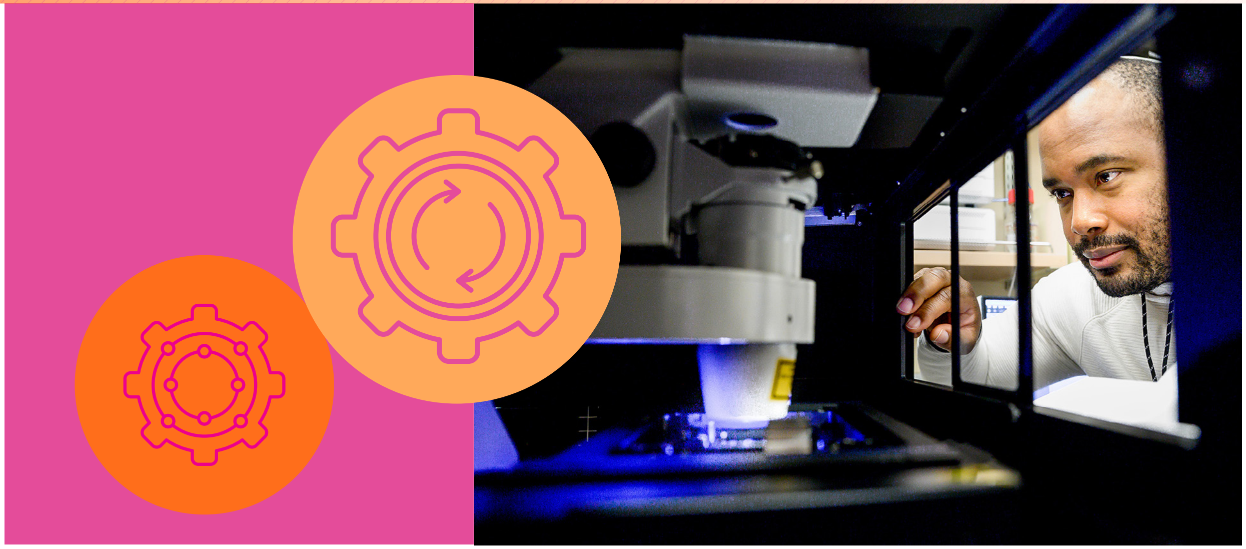
UC SAN FRANCISCO

New Standard Operating Procedure Reduces Compliance Risk

In the spring of 2024, UC San Francisco implemented a new written Standard Operating Procedure (SOP) for reviewing cybersecurity clauses in sponsored research proposals and contracts. The SOP aims to ensure that UC San Francisco meets cybersecurity requirements imposed by sponsors and partners in research contracts, reducing the risk of civil or criminal liability from non-compliance.

The new process is a collaboration between three entities:

1. **The UCSF Office of Sponsored Research Government Contracts Team** handled reviewing, negotiating, and signing sponsored project government contracts (federal, state, and county/city).
2. **The UCSF School of Medicine Technology Services** housed a new Research Cybersecurity Team.
3. **The UC Office of the President's Research Policy Coordination and Analysis** group provided input on the SOP regarding which Federal Acquisition Regulation (FAR) clauses should be flagged for review by the Office of Sponsored Research.



More Efficient Support System

The new approach streamlined support by involving the Office of Sponsored Research, a new dedicated Research Cybersecurity Team engaged directly with grants or contract officers, Principal Investigators (PIs), and sponsors to assess cybersecurity requirements. This streamlined support system helped guide PIs throughout their projects. Additionally, the team retained consultants to conduct a Controlled Unclassified Information review of federal contracts when necessary.

Immediate Impact

The impact of the SOP has been significant, improving contract processing times and reducing compliance risks. PIs receive clear, timely guidance, while contract officers can confidently certify cybersecurity clauses. The campus is now better prepared for external audits, backed by a documented and posted SOP.

The Research Cybersecurity Team has reviewed and provided guidance on eight proposals and contracts so far, with projections to support over 50 annually as demand continues to grow.

UC IRVINE IT ASSET MANAGEMENT SYSTEM

Advancing IT Maturity

With senior leadership championing the initiative, UC Irvine took a bold leap forward in its IT asset management maturity. They faced fragmented inventory management practices across the campus, highlighting the need for a comprehensive, standardized IT asset management system to track IT assets. A multi-functional team, including experts from project management, the data center, and IT departments, collaborated to tackle the challenge. The Office of Information Technology (OIT) spearheaded an initiative in 2022-2023, piloting a proof-of-concept system that laid the groundwork for a campus-wide IT asset inventory system. The pilot aimed to establish a thorough IT asset inventory, implement the system campus-wide, and enable effective asset classification for individual units. After a successful pilot, improvements were made, and the new system went live in June 2024.

The system provides enhanced visibility and control over UC Irvine's IT assets, automatically identifying and tracking both physical and virtual devices connected to the network. Its flexibility allows for manual and batch updates, ensuring comprehensive coverage. With benefits such as reduced security risks, optimized asset utilization, and compliance with IT asset inventory and UC policies, the system is poised to evolve further based on user feedback. As UCI campus units adopt the system, they have increasing real-time visibility into physical and virtual assets, while security teams and campus leadership anticipate reduced cybersecurity threats, improved policy compliance, and stronger governance, setting a new standard for IT asset management across the campus.

TOTAL ASSETS AUTOMATICALLY AND MANUALLY DISCOVERED

29,571

MAXIMIZING RESOURCES

UC's Path to Increased Efficiencies and Impact

In today's rapidly changing landscape, UC must prioritize efficiency by leveraging existing resources and tools while maintaining quality and maximizing impact. By fostering open communication and transparently sharing the "why" behind decisions, UC can align efforts across the institution, driving innovation and growth alongside increased efficiency.

Evolving Together: Streamlining Operations for a Stronger UC

As UC continues to grow and evolve, we remain dedicated to improving and adapting as an institution. With an emphasis on "doing more with less," we implemented organizational restructuring to streamline operations and enhance efficiency. We're continually seeking opportunities to synergize across departments and campuses, ensuring we can meet challenges with innovative solutions and a unified approach.

> *"Safeguarding our systems and data is fundamental to our operational integrity and the trust that our customers place in us. We're embarking on collaborative cross-team projects that enhance our resilience against potential cybersecurity threats.*
>
> **MOLLY GREEK**, Chief Information Officer, Office of the President

Strengthening Resilience: Lessons Learned from Incidents

Each cybersecurity incident offers valuable lessons, resulting in opportunities to enhance efficiency and resilience in our response and prevention efforts. Following a major incident, our remediation efforts first focus on restoring the service, followed by a thorough root cause analysis to understand why the issue occurred. This process often reveals common threads, such as the need to update processes, provide additional staff training, hold vendors accountable or invest in previously under-resourced areas. By addressing these factors, we strengthen our resiliency, reducing the likelihood of similar incidents.

Office of the President: Boosting Security Rating with Minimal Cost

A cybersecurity ratings company evaluates organizations' external vulnerabilities and assigns scores from 250 to 900, similar to a personal credit rating. Executive leadership in Technology Delivery Services (TDS) at the Office of the President set a goal to improve its cybersecurity rating by 10% in 2024, with a stretch goal of 13% by April 2025. To achieve this goal, TDS adopted a new service platform with advanced analytics to better manage risks and fix vulnerabilities. This proactive approach led to measurable improvements without a significant monetary investment while creating a shared sense of purpose among the team.

DIGITAL RISK APPETITE STATEMENT DEFINING AN ACCEPTABLE RISK RANGE FOR UC

To ensure decisions are made using the same parameters of acceptable risk management and to support the roles of UC location Information Security Management Plans, a Digital Risk Appetite Statement was approved by the Board of Regents in March 2024. The statement defines an acceptable risk appetite range and sets expectations of risk management in accordance with best practices and applicable laws and regulations.

Digital Risk is defined as the risk posed from areas such as cyber security, digital accessibility, data privacy, IT third-party risk management, and emerging technology.

⊕ **Digital Risk Appetite Statement**

Cybersecurity Investments: Leadership Awareness and Strategic Action for 2024

The UC President's security letter from February 2024 established systemwide key standards and compliance measures, emphasizing the need for cyber investment plans to support these requirements. With robust support and increased leadership awareness of cybersecurity risks, these investments are critical for strengthening security across the organization.

UC Security Leaders Named as Finalists for the Bay Area CISO ORBIES Awards

The ORBIE Awards honors CISOs who have demonstrated excellence in technology leadership. Over 500 leaders have received an ORBIE Award since its inception in 1998.

> *The most challenging part of being a CISO is there are no guarantees. Answering, 'Are we secure?' is tough, no matter the investment or talent. Staying ahead of threat actors is always challenging, especially with the rise of AI and advanced computing.*
>
> **APRIL SATHER**, CISO, Office of the President

April Sather, CISO, Office of the President

NOMINATED IN THE ENTERPRISE CATEGORY

Career: April spent her early career in various positions at Deloitte, Sun, Computer Sciences Corporation, and First West Credit Union before serving as Chief Information Security Officer and Director, Innovation, Architecture, and Security Services at Pacific Blue Cross. In 2019, April joined UC Irvine as Assistant CISO before becoming CISO at the Office of the President in 2022.

Education: April earned her MBA from UC Irvine and her Bachelor of Information Technology & Commerce from Bond University, Australia.

Favorite Thing About Being a CISO: Building and executing strategy in the critical space of cybersecurity is incredibly rewarding. I enjoy the fast pace and working with teams to implement processes and technologies that reduce risk. Being a CISO allows me to build trust across the organization and position security as an enabler of mission and innovation, not a blocker.

Favorite Things to Do Outside of Work: Travel and adventures with my family are at the top of my list. I also love exploring new cuisines and food experiences, replicating these at home with varying levels of success.

Allison Henry, CISO, UC Berkeley

NOMINATED IN THE LARGE ENTERPRISE CATEGORY

Career: Allison started her information technology career as a system administrator at UC Santa Cruz. In 2004, she joined Communications and Network Services at UC Berkeley, pivoting to information security in 2006. In 2013, Allison started managing the Security Operations team. In 2018, she served as Associate CISO before assuming the role of CISO in December 2019.

Education: Allison graduated from UC Berkeley with a Bachelor of Science in Integrative Biology in 1996.

Favorite Thing About Being a CISO: It's a rewarding career that offers daily challenges, a meaningful purpose, and authentic human connection.

Favorite Things to Do Outside of Work: In addition to information technology and security, I have a passion for the study of optimizing human performance through fitness and nutrition. I enjoy endurance athletics, including running and cycling.

Annual Data Disposal Day at UC Irvine Safeguards Information and Community

One of the most anticipated events of the year at UC Irvine is Data Disposal Day, a dedicated initiative for the secure disposal of paper and electronic data devices. This year, hundreds of community members from across the campus participated, bringing in used boxes of documents and electronic media to be sorted and securely destroyed. "Data Disposal Day is an extremely popular event," shared Josh Drummond, UC Irvine's Chief Information Security Officer (CISO). "We get requests to do it again just weeks after the event."

Disposing of institutional information requires careful handling to prevent unauthorized access or accidental disclosure of sensitive data, which bad actors could exploit. The UC Institutional Information Disposal Standard offers guidance on how to properly dispose of data based on its risk level, from very low-risk data (P1) to very high-risk data (P4). For example, a thumb drive containing P1 data can simply be deleted, while one containing P4 data must be securely erased or destroyed. Additionally, this process must align with the UC University Records Management Program (BFB-RMP-1) and the UC Records Retention Schedule.

⊕ UC Institutional Information Disposal Standard
⊕ UC University Records Management Program
⊕ Records Retention Schedule

DATA DISPOSAL DAY
with Southern California Shredding
ZotDefend
Cybersecurity Awareness Month

> *It's easy to forget what sensitive information might be on an old hard drive or document. Proper disposal is crucial to protect you, your family, and the university from data breaches.*
>
> **JOSH DRUMMOND**, CISO, UC Irvine

2024 DATA DISPOSAL DAY BY THE NUMBERS

18,000+
pounds of shredded paper, almost filling 2 large trucks

1,790+
hard drives destroyed

860+
other media (phones, tablets, floppy disks, CDs, and various other data storage gadgets) destroyed

Volunteers for the Data Disposal Day gather beside some of the many items ready for safe disposal.

Policy Corner

The intersection of governance and compliance, driven by emerging standards and external factors, poses significant challenges for our tools and systems. Our policies will continually adapt to meet these evolving requirements.

COMPLIANCE Graham-Leach-Bliley Act

The Graham-Leach-Bliley Act (GLBA) exemplifies the intersection of compliance and governance. GLBA requires institutions that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and safeguard sensitive data. One of the requirements calls for a written report of an information security program.

GLBA Survey and Report Update: To fulfill the requirement of a written report, a survey was created for the UC locations, which was completed in 2023 and updated in 2024. The survey included existing implementations that meet GLBA requirements, as well as areas for improvement. Based on the results, reports containing the full picture of GLBA compliance across UC locations were developed.

UC Location Plans for GLBA Compliance: To meet obligations under GLBA, UC locations developed compliance plans. For example, UC Berkeley's plan includes a custom-built risk registry and action plans for impacted systems.

RESOURCE UPDATES

In the spirit of continuous improvement, the following documents were revised based on tabletop exercises in 2022 and 2023, as well as feedback from multiple stakeholders in the process.

- Systemwide Cyber Incident Response Process This document defines the systemwide cyber incident response coordination process at UC.
- Cyber Incident Escalation Protocol and Guidance The document provides revised guidance on implementing the Cyber Incident Escalation Protocol.

Continued →

SPOTLIGHT UC Berkeley Integrated Campus Units Into the IS-3 Risk Management Program

In partnership with the entire campus community, the Information Security Office (ISO) at UC Berkeley completed a 4.5-year initiative to integrate all central IT, academic, and administrative units into the campus IS-3 cyber risk management program. UC Berkeley's Cyber Risk Management Program is a holistic program that helps units manage their cyber risk and comply with IS-3, UC's systemwide Electronic Information Security Policy.

This project was focused on raising awareness among Unit Heads and Unit Information Security Leads (UISLs) about their roles and responsibilities related to information security and providing units with concrete, unit-specific, prioritized recommendations on how to address areas of highest risk. Throughout the project, the emphasis was on risk awareness and risk management, providing value to the unit, building relationships, and incremental progress over time. Onboarding started in 2020, and the final cohort wrapped up in 2024. The team shared the work at the annual UC Tech Conference in a presentation entitled UC Berkeley's IS-3 Risk Assessment Journey.

2025 Next Steps

In 2025, this project will transition to an ongoing, operational program of regular reviews and updates, continuing to focus on addressing areas of highest risk; measurable, incremental improvement over time; and maintaining relationships. The operational program will also include an annual theme that focuses on a key risk area relating to IS-3. These themes will provide information, resources, and tools, such as services and templates, to help units make progress in the focus area. Over time, ISO envisions having a robust suite of tools and services to help units manage their information security risk.

⊕ **IS-3 Cyber Risk Management Program**
⊕ **IS-3, UC's systemwide Electronic Information Security Policy**
⊕ **Cyber Risk Management Program Service**

OUTCOMES

- ISO identified 84 academic and administrative units, met with every Unit Head and UISL, and worked in cohorts through a facilitated process of asset inventory and high-level security self-assessment.
- The units completed, and ISO reviewed, a total of 95 unit self-assessments.

KEY PROGRAM PRINCIPLES

Security Is a Shared Responsibility: EVERYONE HAS A ROLE

Protection Level and Availability Level INFORM RISK LEVEL AND CONTROLS

Focus on Risk Management; RISK ASSESSMENT IS KEY

Units Are Responsible for Managing Their Own INFORMATION SECURITY RISK

Navigating the Evolving Threat Landscape

The cybersecurity landscape at UC remained focused on addressing evolving threats, leveraging security AI/automation, and incident response testing to strengthen defenses. Collaboration across campuses and health systems fostered a systemwide security mindset. As we look to the future, UC looks to cybersecurity predictions to stay ahead of emerging threats and better prepare for the challenges ahead.

RISKS AT A GLANCE

$4.88M average cost of a data breach

180% increase in the exploitation of vulnerabilities as an initial attack vector

90% of breaches in the education services industry stem from social intrusion, social engineering, and miscellaneous errors

68% of breaches are driven by the non-malicious human element (Note: Verizon now looks at non-malicious human elements, not just any human activity)

23% of attacks are linked to ransomware

16% of breaches are due to compromised credentials—the most common attack vector—with an average cost of $4.81M

15% of breaches are linked to phishing, with an average cost of $4.88M

15% of data breaches involve supply chains

< 60 Seconds is the median time for a person to fall for a phishing email

BENEFITS AT A GLANCE

98 Days Saved Organizations extensively using security AI and automation identified and contained a data breach faster than organizations with no usage

84 Days Saved Attack Surface Management (ASM) helped accelerate the total time to identify and contain a data breach by nearly 12 weeks

28 Days Saved Organizations using threat intelligence identified breaches 28 days faster than those without

$2.2M decrease in breach costs when using AI and automation in prevention workflows

$258K decrease in average breach cost when organizations implemented employee training the most effective data breach cost mitigator

CHANGES FROM 2023 TO 2024

15% increase in internal threat actors in breaches

13.1% increase in data breaches in public clouds, costing an average of $5.17M

11% increase in lost business and post-breach response costs

10.6% decrease in the average breach cost for healthcare to $9.77M

10% increase in the global average cost of a data breach—the largest spike since the COVID-19 pandemic

10% increase in the use of AI and automation in security operations

SOURCES:
IBM Cost of a Data Breach Report 2024, IBM Security.
Verizon Data Breach Investigations Report 2024.

Interactive Learning Pavilion

UNIVERSITY
OF
CALIFORNIA

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

We are excited to announce that the Cyber-risk Coordination Center (C3) is now UC Digital Risk and Security. This change reflects our expanded focus on digital risk management and security across the UC system.