2025 ANNUAL REPORT

UC's Digital Impact Engine

Celebrating a year of innovation, cybersecurity, and operational excellence

UNIVERSITY OF CALIFORNIA

Table of Contents

Introduction

Innovation

Digital Risk and Cybersecurity

Operational Excellence

Introduction

This is the first annual report from Digital Innovation & Technology, bringing together innovation, cybersecurity, and operational excellence in one place to show how technology advances UC's mission as a whole.

INNOVATION

Innovation at UC is increasingly defined by how well we connect people, platforms, and ideas across a complex system. This section explores how Digital Innovation & Technology (DigIT) is evolving to meet that challenge—advancing responsible AI, strengthening governance, enabling systemwide dialogue, and building new partnership networks that accelerate impact. Together with a snapshot of DigIT by the numbers, these stories illustrate how thoughtful investment, collaboration, and strong digital foundations are enabling UC to innovate at scale while supporting its academic, research, and public missions.

CYBERSECURITY

Cybersecurity is foundational to UC's ability to innovate, teach, and serve the public with confidence. This section highlights how the University is strengthening its digital resilience in the face of a rapidly evolving threat landscape through systemwide collaboration, strategic investment, and leadership-driven action. From improving security performance and meeting ambitious compliance goals to addressing AI-powered threats and protecting research and healthcare environments, these stories reflect UC's shared commitment to safeguarding its people, data, and mission at scale.

OPERATIONAL EXCELLENCE

Operational excellence is how we translate strategy into day-to-day reliability for the people and programs UC serves. This section reflects on a year—and a leadership chapter—focused on making our work more visible, our services more people-centered, and our stewardship more disciplined. The stories that follow highlight how Technology Delivery Services is strengthening foundations, modernizing core processes, and applying practical AI to reduce manual work and improve responsiveness. From resilient infrastructure and smarter supplier and financial systems to service design and accessibility, the goal is consistent: technology that works reliably, responsibly, and in service of people.

Welcome

This year marks an important milestone for our organization. As we look ahead to UC's digital future, we have adopted a new name—**Digital Innovation & Technology (DigIT)**. This change reflects more than a shift in branding; it reflects what our organization has become and the direction we are heading. Technology is now inseparable from every part of the University of California's mission, and our identity is evolving to match the scope, reach, and ambition of our work.

Over the past year, we have been making thoughtful, incremental changes to align our structure and work with our vision of becoming *UC's digital impact engine*. We are strengthening the systems and platforms that power the university, expanding our focus on digital experience and service design, and building new capabilities that enable innovation across teaching, research, health, and administration. These shifts position us not only as stewards of core infrastructure, but as strategic partners helping shape UC's future.

At the same time, we recognize the very real headwinds facing higher education. Challenging budgets, rising complexity, and declining public trust make our work both harder and more essential than ever. In moments like these, technology's role becomes even more critical: enabling efficiency, strengthening resilience, improving outcomes, and helping restore confidence in our institutions. Our interconnected UC system is uniquely positioned for this moment—its diversity fuels experimentation, creativity, and local problem-solving. Our job at DigIT is to help connect those efforts, amplify what works, and create the conditions for digital progress across the system.

I am grateful for the talent and dedication of our DigIT team and for the partnerships across UC that make this work possible. With our new name and renewed focus, we look forward to partnering with campuses, labs, and health systems to imagine and build the next chapter of UC's digital story.

VAN WILLIAMS
Vice President of DigIT and Chief Information Officer, University of California

Digital Innovation & Technology advances the University of California's mission by strengthening core systems, enabling responsible innovation, and connecting people, platforms, and partners to deliver reliable, secure, and people-centered digital services at scale.

Digital Innovation & Technology Leadership

KRISTIN CORDOVA
Chief of Staff, Immediate Office

INNOVATION

Delivering Enterprise IT Within Budget

The IT department demonstrated strong financial discipline while sustaining delivery of critical services and advancing priority initiatives.

During the fiscal year, IT managed a $92.5M operating budget and closed the year with $89.3M in expenditures—$3.2M under budget—reflecting deliberate planning and active portfolio oversight.

Spending remained appropriately weighted toward people, with 83% of the budget invested in the workforce responsible for operating, securing, and modernizing enterprise systems, and 17% supporting the platforms and services that enable campus operations. This approach ensured fiscal accountability while maintaining the capacity to adapt to shifting timelines and organizational needs.

Digital Innovation & Technology by the Numbers

SECURITY

86.18% Microsoft Secure Score (40% better than peer organizations)
10–15K Threats on email blocked daily
200K Emails protected daily

$73.8M
People-related labor costs

$15.5M
Operational (non-labor) costs

248
Full-time staff

61
External contractors

278K
Sensitive files in Box protected

160 SEV-1
Major incidents resolved

190
Applications supported

715
Total managed assets

2.3M
Authentications a month

477K
Zoom meetings

UC's AI Strategy: Leading Higher Education Into an AI-Enabled Future

The University of California has set a bold goal: to become higher education's leader in AI. Across ten campuses, six academic medical centers, and three national labs, UC's varied ecosystem creates a vibrant environment for diverse experimentation, rapid prototyping, and locally driven innovation. Systemwide collaboration and knowledge sharing generates a rich network of use cases, insights, and community that strengthen the whole.

UC's AI strategy clarifies priorities, highlights shared opportunities, and guides sound investments rather than prescribing a uniform implementation path. It provides a common language and direction, enabling locations to learn from one another, build on emerging successes, and collectively advance responsible and impactful uses of AI. The strategy's foundation is rooted in established governance on the responsible and ethical use of AI, and the vision is organized around three pillars.

1

Scaling Innovation

- Expanding responsible access to generative AI tools for faculty, staff, clinicians, and researchers.
- Enabling diverse campus experimentation—from syllabus generation and tutoring to ambient listening in clinical settings and research computing.
- Building a growing portfolio of proofs of concept that strengthens UC's foundation for systemwide innovation.

2

Fostering Strategic Partnerships

- Deepening collaborations with major technology partners for expertise, infrastructure, and educational support.
- Expanding engagement with state and federal agencies on AI policy, risk, and workforce development.

3

Preparing California's Workforce

- Partnering with industry and state agencies to align workforce preparation with evolving labor market needs.
- Expanding pathways for reskilling and upskilling through continuiing education programs.
- Contributing research and expertise on AI's impact on work, helping shape statewide workforce development strategies.

Steering UC's Responsible AI Journey

Effective governance and collaboration are essential as we expand AI's role across the University of California system. Here is a snapshot of the key bodies guiding the work.

UC AI Council

Chaired by senior academic and administrative leadership and composed of representatives from all UC locations and disciplines, the UC AI Council develops systemwide guidance for the responsible adoption of artificial intelligence, including risk and impact assessment processes and transparency frameworks. The Council promotes information and resource sharing across university operations through coordinated training, outreach, and awareness initiatives.

AI Executive Steering Committee

As a high-level oversight group, the Steering Committee provides strategic direction and prioritization of AI initiatives, helps align investments and coordination across the enterprise, and ensures alignment with the broader mission of UC.

UC AI Strategic Leaders Community of Practice

Started in 2025, the systemwide forum brings together campus leaders at the intersection of AI strategy and operations. Its goals are to surface promising use-cases across campuses, enable cross-campus knowledge exchange and training on operational AI applications, and share strategies for responsible adoption, including governance, risk, change management, and capacity-building.

These groups, along with the many communities emerging at different locations, help enable distributed experimentation, informed coordination, and shared learning across UC's complex environment.

Connecting UC for an AI-Ready Future

DEPLOYING AI
UNLOCKING the STRATEGIC POTENTIAL, AVOIDING PITFALLS, and GETTING the ORGANIZATION ----READY-->
EXPERIMENTATION
IN THE RIGHT FASHION
CAMERA TURNS ON WHEN TALKING TO CHAT BOT
ALGORITHM THAT READS HUMAN EMOTION
DEPARTMENT WIDE USE ?
VALUE PROPOSITION
AI CANNOT BE A HUMAN... ...YET
MAYBE IT'S NOT COST EFFECTIVE
ORGANIZATIONAL CHALLENGES
• SECURITY
• SAFETY
• DATA QUALITY
• ETHICS
• PRIVACY
HAVE A CLEAR VALUE PROPOSITION
A.I. ENABLING Culture
TRANSFORMING YOUR ORGANIZATION
TALENT GAP
LEADERSHIP VISION & STRATEGY
LONG-TERM ADVANTAGE?
WHY PRIORITIZE?
ALIGNMENT
GET YOURSELF READY
FRAMEWORK
FOR GAUGING YOUR AI ADOPTION READINESS
III
IV
BUILD AND IMPLEMENT
I
WAIT FOR THE RIGHT TIME
II
NO BETTER SYSTEM THAN THE UCs
Saikat Chaudhuri
UC Berkeley
LEARN FROM EACH OTHER
I DON'T ASK FOR PERMISSION
I ASK LATER FOR FORGIVENESS!
I CAN GET STUFF DONE FASTER NOW MORE THAN I WOULD HAVE IN THE PAST!
PITFALLS
3 NOT EXPLORING ITS TRANSFORMATIVE POTENTIAL
5 IMPLEMENTING WITHOUT A GOOD VALUE PROPOSITION
LEGO FOOTWEAR ON THE MANUAL
WHAT ACTIONS MIGHT YOU TAKE NEXT?
GO ON!
WHERE DOES YOUR ORGANIZATION CURRENTLY STAND?
EVIDENCE BASED MINDSET
IMPROVEMENT
UNIVERSITY OF CALIFORNIA

Following the success of the 2024 UC Academic Congress on AI, the UC AI Council and the UC Chief Information Officer Council convened a workshop titled *"Creating a Smarter University: AI Transformations in Administration"* at the UCLA Luskin Conference Center on September 30 – October 1, 2024. The invitation-only gathering brought together senior administrative leaders across the UC system to explore how AI can drive innovation in enterprise operations, academic support, research infrastructure, and healthcare administration.

Highlights included keynote and panel sessions that addressed AI-driven innovation, governance, scaling use cases, and institutional readiness. Breakout workshops invited participants to build strategic AI roadmaps, pilot programs, and governance models. And an interactive Share Fair showcased real-world AI projects from across campuses, ranging from chatbots and VR recruitment to accessibility tools and workplace-safety analytics. The event was a catalyst for continuing dialogue and action on integrating AI effectively into administrative ecosystems across UC.

Key Takeaways

AI is moving from experimentation to strategy

UC leaders are shifting from one-off pilots to coordinated, scalable approaches supported by shared frameworks and governance.

Collaboration is essential for systemwide progress

Cross-campus knowledge sharing and reuse of proven use cases are key to accelerating responsible AI adoption.

Readiness matters as much as innovation

Effective AI implementation requires strong foundations in governance, policy, risk management, and workforce training.

Building Partnerships to Drive Digital Transformation: The Digital Innovation Partnership Network

The Digital Innovation Partnership Network (DIPN) is a new initiative designed to drive digital transformation by connecting UC campuses and health centers with external partners across industry, government, and philanthropy. The network facilitates collaboration on bold ideas, scalable pilots, and inclusive innovation that will benefit students, faculty, and communities across California and beyond.

The work will align with and support the priorities of key internal stakeholder groups, from research and IT to student success and sustainability. These groups are critical to identifying needs, co-developing pilot opportunities, and activating partnerships that have real impact across the UC system. External groups include:

- Federal, state, and local government agencies
- Industry and private sector partners (tech, healthcare, infrastructure, etc.)
- Foundations and nonprofits
- Research institutes and education networks

Opportunities fall into four strategic categories:

Talent & Workforce
Workforce development, student engagement, teaching & academic support, degree plus expansion support

Social & Public Impact
Collaboration on public interest policy, K-12 pipeline development, community outreach & engagement

Strategic Visibilty
Event sponsorship & co-branding, philanthropy & strategic giving, advisory & thought leadership

Research & Innovation
Research collaboration, innovation, & entrepreneurship

Driving Innovation, Transforming Security

As we reflect on another year of progress, the University of California continues to strengthen its digital resilience through bold, innovative approaches to digital risk.

This year's report reflects the evolving digital risk landscape and highlights how UC's efforts, backed by strong leadership, are shifting from awareness to more strategic action.

The stories highlight UC's forward-thinking strategies—from launching collaborative privacy initiatives to expanding systemwide tools. Campuses and departments are coming together to protect UC's digital assets, share insights across higher education, and build a culture of cybersecurity awareness. While we can't capture every milestone here, the report reflects the momentum, innovation, and commitment to excellence that define UC's cybersecurity journey.

We also want to recognize the tremendous effort made by every UC location in meeting systemwide cybersecurity requirements. These achievements reflect not just compliance, but a shared dedication to safeguarding the University's mission and integrity. Thank you to everyone who contributed to this year's progress—your work is foundational to UC's future. Let's continue building on this momentum together.

MONTE RATZLAFF
UC Chief Information Security Officer
Office of the President

Within Digital Innovation & Technology, UC Digital Risk and Security partners with UC locations to strengthen cybersecurity, privacy, and risk management across the system, providing leadership, coordination, and shared capabilities that protect UC's people, data, and mission in an evolving threat landscape.

UC Digital Risk and Security Leadership

APRIL SATHER
Interim Systemwide Cyber Defense Officer,
Chief Information Security Officer,
Office of the President

2025: The Cybersecurity Landscape by the Numbers

$3.8M

The average cost of a data breach in the education industry went from $3.5M to $3.8M from 2024 to 2025.

$7.4M

Healthcare remained the most expensive industry for breaches for the 12th consecutive year—even as it saw a sharp reduction from last year ($9.77 million).

267 days

Third-party vendor and supply chain attacks took the longest to detect and contain—an average of 267 days in 2025.

16%

Attackers are using AI to manipulate humans.

Researchers found 16% of breaches involved attackers using AI.

32%

Reporting a breach to regulators and other government agencies has become a common part of post-breach responses.

This year's report found about a third of organizations paid a regulatory fine because of breaches.

62%

External actors (individuals or groups outside of an organization) are behind 62% of the attacks in the educational services vertical.

59% of those actors are associated with organized crime.

SOURCES: IBM Cost of a Data Breach Report 2025, IBM Security. Verizon Data Breach Investigations Report 2025.

Building a Stronger Security Foundation Across UC: The President's Information Security Investment Plan Letter

Across the University of California, teams worked tirelessly to achieve the cybersecurity objectives set forth by then-President Michael V. Drake. Driven by increasing threats and incident costs, the President's information security investment plan aimed to address cybersecurity vulnerabilities and compliance risks by meeting six key objectives in both standards and controls compliance.

This effort would not have been possible without dedicated teams working systemwide to meet the challenge. From campus IT professionals to executive leadership, each contributor played a vital role in moving the program forward and advancing UC's security goals.

UC has established a robust foundation for a resilient cybersecurity program through strategic investments, resulting in a safer digital environment for everyone. UC locations will continue to strengthen this work, supported by the Office of the President through clear accountability, transparent reporting, shared infrastructure, and cross-functional coordination.

This achievement reflects the collective dedication and collaboration of teams across the University of California. These efforts demonstrate the strength of our systemwide community and the vital role cybersecurity plays in protecting UC's mission and values.

> *"The chancellors and their teams were instrumental in significantly strengthening UC's security posture, and we're grateful for everyone's commitment in achieving these objectives."*
>
> **MONTE RATZLAFF**
> **UC Chief Information Security Officer**

Outcome	Impact
Ensure cyber security awareness training for 100 percent of location employees.	Improved training compliance, boosting cybersecurity awareness and accountability across UC.
Ensure timely cyber escalation of incidents in alignment with UC Incident response and cybersecurity escalation standards.	Reinforced importance of rapid incident reporting.
Ensure identification, tracking, and vulnerability management of all computing devices connected to university networks.	Increased accuracy in IT asset inventory and improved remediation of system vulnerabilities.
Deploy and manage UC-approved Endpoint Detection and Recovery (EDR) software on 100 percent of assets defined by UC EDR deployment standards.	Enhanced endpoint security and VPN access control by deploying EDR on 100% of in-scope assets.
Deploy, enable, and configure multifactor authentication (MFA) on 100 percent of campus and health email systems in conformance with established UC MFA configuration standards.	Extended MFA to all email systems and increased consistency in MFA configurations.
Deploy and configure a robust Data Loss Prevention (DLP) solution for all health email systems to mitigate unauthorized data exfiltration.	Reduced risk of unauthorized sharing of protected health information (PHI) via email using advanced data loss prevention technology.

Strengthening Research Security Across the UC System

As part of its commitment to protecting the integrity of academic research, the University of California continues to strengthen its research security practices systemwide. The urgency around safeguarding research is more pressing than ever due to pervasive cybersecurity threats and increased oversight and compliance expectations for federally sponsored research at higher education institutions.

One example is the Research Security and Cybersecurity Maturity Model Certification (CMMC) Working Group, formed to address research security. Co-chairs Jason Christopher (Research IT - UC Berkeley) and Melonie White (UC Digital Risk and Security - Office of the President) are leading the group to better understand campus experiences with research cybersecurity and framework compliance. Through collaboration and information sharing, the group has identified challenges in key areas systemwide. The team will share the findings with leadership to help inform future discussions, further collaboration between locations to support research, and advise on potential next steps.

AI Vetting: Balancing Innovation and Risk

While the rapid rise of AI tools brings opportunities, it also ntroduces security, legal, and privacy risks. Across the UC system, a team of cybersecurity and digital risk experts helps leadership navigate these risks through a thorough risk analysis process.

The AI vetting process begins with an AI Security Risk Assessment (AI SRA), which builds on UC's existing supplier review program. Privacy and legal assessments complete this three-part review. The AI SRA process involves in-depth conversations with vendors and a deep dive into each tool's architecture to understand how it handles UC data and prevent its use in model training. Damian Luna, Cyber Risk Unit Manager, Office of the President, said, "We present leadership with the risks we uncover to help them make more informed choices about cutting-edge technology like AI."

The team faces multiple challenges, including getting to the heart of what's behind an AI product and managing vendors' reluctance to reveal information while keeping pace with rapidly changing technology and client needs. "Oftentimes, vendors don't want to share details about the inner workings of their product," explained Eric Hull, Manager, IT Security, Office of the President. "But understanding those details is exactly what helps UC protect its data. We try to help people achieve what they want, but we need to do so in a way that's safe for the institution. And that can take time and perseverance."

One recent review is a perfect example of why this work is so critical. The team's assessment of a popular AI transcription tool uncovered significant security and privacy concerns. The security, legal, and privacy teams recommended not using the tool in favor of the already-vetted supplier and product that provide similar services under the current license. The AI company later faced legal scrutiny over its data practices.

As AI evolves daily, so does UC's approach to managing it. By balancing innovation with vigilance, the team's ability to stay nimble empowers UC to confidently advance while protecting UC's data, research, and people.

UC San Diego Redefines Cybersecurity in Healthcare

Photo credit: Kyle Dykes/UC San Diego Health Sciences

The UC San Diego Cyber Health initiative has emerged as a national leader in understanding and mitigating the real-world impacts of cyberattacks on healthcare delivery.

Through groundbreaking research, the team, led by Christian Dameff, M.D. and Jeffrey Tully, M.D., demonstrated how ransomware attacks on one hospital system can ripple across adjacent, untargeted facilities—leading to longer emergency department wait times and reduced survival outcomes.

Their studies show that cyber disruptions are not isolated IT issues but public health emergencies that demand coordinated disaster response planning across regional healthcare systems.

Dr. Dameff shared his thoughts on some key questions.

Your research shows that cyberattacks can lead to real-world health consequences. What was the most surprising or alarming finding from your studies?

Ten years ago, we had no evidence that cyberattacks were impacting patients. Everyone knew it was happening—we had all these horrible stories people were telling—but there wasn't good research to quantify it or better understand it. One of the most surprising things about our research, which shows that cyberattacks can impact patient safety and well-being, is that we've only scratched the surface. Every time I talk to another doctor or nurse who cared for patients during an attack, they share another impact I had never even thought about. We have yet to even begin to understand how big a problem this is.

UC San Diego Redefines Cybersecurity in Healthcare (con't.)

Photo credit: Susanne Clara Bard/UC San Diego Health Sciences

Visit the UC San Diego Center for Healthcare Cybersecurity website to learn more.

UC San Diego is pioneering the field of Cyber Disaster Medicine. Can you explain what that is, and describe what role it should play in future emergency preparedness training for healthcare professionals?

Cyber Disaster Medicine applies principles from traditional disaster medicine to cyberattacks, recognizing that caring for patients during these events is different from normal conditions. While lessons from natural disasters help, cyberattacks are unique—they involve intelligent, motivated adversaries, occur without warning, lack geographic patterns, and can last for weeks or months. Unlike hurricanes or wildfires, there's little forewarning, and hospitals everywhere are vulnerable. This emerging field aims to close research gaps, share best practices, and develop strategies to protect patients during prolonged, unpredictable cyber crises.

Please share an example of how a hybrid response model combined with traditional incident command systems with modern IT playbooks was successfully implemented or tested.

Hospitals have strong plans for natural disasters but cyberattacks are rarely included. Emergency managers lacked training for ransomware events, while IT teams had technical recovery plans—creating a gap in coordinated response. To address this, new clinical playbooks have been developed to guide care during cyber incidents, covering critical scenarios like heart attacks, strokes, and cancer treatments. The goal is to minimize patient harm and maintain care quality during prolonged cyber crises. This initiative is in its early stages; next steps include adoption, contributions from clinicians, and continuous updates to create an international standard supported by the best available science.

What steps can hospitals and regional healthcare systems take today to better prepare for the ripple effects of a cyberattack—even if they're not the direct target?

Ransomware attacks affect not only the targeted hospital but also surrounding facilities, increasing strain and wait times. The best defense is proactive planning: hospitals should form regional coalitions, share resources, and establish agreements for patient diversions and technical support before an attack occurs. Communication and tracking systems are critical since outages can last weeks or months.

UCLA Chief Data and AI Officer Warns of AI-Powered Cyberattacks

The Deepfake Dilemma

AI-driven cyberattacks, particularly deepfakes and automated phishing, are reshaping digital risk in higher education. AI-generated videos, images, and audio impersonations can convincingly mimic trusted individuals, leading to identity theft, fraud, and reputational harm. AI also powers sophisticated phishing and social engineering attacks, making them more personalized and harder to detect.

According to Chris Mattman, UCLA's Chief Data and Artificial Intelligence Officer (CDAIO), these tactics represent the biggest threats to universities and students today.

"Students are particularly prone to such cyberattacks as deepfakes, as they are online quite a bit," Mattmann said. "But, no one is immune," he continued. "Look at what happened to Secretary of State Marco Rubio."

In the summer of 2025, attackers used a deepfake of Rubio to impersonate him via text, voicemail, and the messaging app Signal—reaching foreign ministers, a senator, and a governor.

Combatting Threats

Mattmann stresses the importance of digital literacy and cybersecurity education, noting that awareness and training are essential to recognizing and responding to AI-powered threats. He also emphasizes the need for layered, AI-powered infrastructure, like firewalls, traffic scrubbing, and real-time anomaly detection, to proactively block threats.

By implementing AI-powered tools and real-time anomaly detection, the emerging UCLA's Bruin Connect and Secure program is enabling UCLA to proactively detect and block cyber threats before they impact the community. The modernized network not only responds in real time but also continuously improves by learning from past attacks.

> **Learn more about AI-driven defense strategies in Chris Mattman's conversation with UC Net.**

Think you can spot fake accounts?
Take the SpottheTroll.org quiz

Security Performance Management Platform Helps Improve Defenses Across UC

In 2025, the Office of the President significantly strengthened its cybersecurity posture by significantly improving its BitSight rating — a clear reflection of enhanced security hygiene and resilience.

Led by April Sather, Office of the President Chief Information Security Officer (CISO) and Interim Systemwide Cyber Defense Officer, the UC Digital Risk and Security team worked with various teams across the Office of the President to address critical vulnerabilities. The teams also stengthened the multifactor authentication process to better protect institutional assets and data.

In a significant move toward systemwide alignment, the Office of the President began funding the BitSight platform for each UC location to use. This tool will enable campuses and departments to independently monitor their cybersecurity performance using a standardized, data-driven framework.

By extending access to the BitSight platform and elevating security practices across the system, the Office of the President is helping ensure that every campus can protect critical assets while advancing the University's mission. A stronger, more resilient cybersecurity posture enables UC to pursue innovation, collaboration, and discovery with confidence.

The Office of the President's BitSight Rating Improved 20%

A BitSight rating works like a credit score, where higher is better. A high rating means it is tougher for attackers to gain access.

2025 Cybersecurity Summit Focused on Security and Innovation Across Higher Ed

On August 19–20, 2025, more than 800 attendees from the University of California, California State University, and California Community Colleges gathered virtually for the 16th UC Cybersecurity Summit. Centered on the theme "Building Resilient Communities," the event fostered collaboration and knowledge-sharing across institutions.

Moderated by Monte Ratzlaff, UC Chief Information Security Officer, the summit featured speakers from prestigious institutions including Stanford, Harvard, the University of Texas system, University of Oregon, and the U.S. Secret Service—bringing together diverse perspectives to strengthen cybersecurity across higher education.

The summit tackled key cybersecurity issues, from AI-driven threats and privacy to ransomware resilience and cloud security, emphasizing that cybersecurity is a strategic leadership priority in higher education.

The summit underscored the power of collective learning and collaboration, affirming that building resilient communities across UC begins with working together, sharing knowledge, and strengthening our collective defense against emerging threats.

Read the event wrap up on UC Tech News: 2025 Cybersecurity Summit Highlights

2025 Cybersecurity Summit Speakers and Presenters

NANDITA BERY, Director of Cybersecurity, Equinix

JENNIE KENNEDY, Chief Privacy and Data Protection, University of Texas

SUNNY NOTANI, Special Agent, US Secret Service

DR. CHRIS MATTMANN, Chief Data and AI Officer, UCLA

DR. NEIL DASWANI, Co-Director, Stanford Advanced Cybersecurity Program

MICHAEL TRAN DUFF, Chief Info Security & Data Privacy Officer, Harvard

DR. KEITH CLEMENT, Professor, California State University

JOSH CALLAHAN, CISO, California State University

CHRISTY LONG, Associate CIO and Chief of Staff, University of Oregon

DRAKE CHANG, CISO, UCLA

93% of post-summit survey responders said they were satisfied/very satisfied with the virtual experience

Serving UC Through Thoughtful Technology

In this annual report, I am not only reflecting on the year but also reflecting on my time at the Office of the President and the work we have done together. This will be my final year reporting in this role, and it feels fitting to pause and acknowledge both the progress we have made and the people who made it.

Throughout my tenure, I believed strongly in the value of clear, consistent communication. The introduction of quarterly newsletters and the evolution of the Technology Delivery Services (TDS) Annual Report were intentional efforts to make our work more visible and to tie our effort to the mission that all of us are focused on. Much of what TDS does happens behind the scenes, yet it directly affects how the University operates every day. Our goal is to build trust, strengthen partnerships, and help all of you be successful. Your success is our success.

Coming to the Office of the President from a UC Health location broadened my perspective about UC and how we serve the state and the country. The University of California is not only complex, but also deeply impactful. The work done here supports students, faculty, researchers, clinicians, and staff across the state. The Office of the President plays a critical role in enabling that work, and serving in this capacity has been a privilege.

Operational excellence and service have guided my approach. Whether improving customer experience, strengthening stewardship of resources, or building resilient and secure systems, the goal has always been the same: ensure technology works reliably, responsibly, and in service of people.

This section of the report highlights that commitment in action. While leadership transitions are a natural part of an organization's evolution, the foundation we've built together is strong. I am confident in the teams who will continue this work and in UC's ability to move forward with focus and purpose.

It has been an honor to serve UC with all of you.

MOLLY GREEK
Office of the President Chief Information Officer
UC Digital Innovation & Technology

Within Digital Innovation & Technology, Technology Delivery Services ensures the reliable delivery and operation of UCOP's core technology services, focusing on infrastructure, applications, service management, and operational excellence that keep essential systems running securely and efficiently every day.

Technology Delivery Services Leadership

KARI ROBERTSON
UCOP Deputy Chief Information Officer
and Chief Technology Officer
UC Digital Innovation & Technology

Aligning Strategy, Delivery, and Customer Experience

This year, Technology Delivery Services formed two new teams to better align strategy, delivery, and experience in support of reliable, people-centered services.

Product, Project and Service Management

This team brings product stewardship, project coordination, and service management together to guide IT services from strategy through delivery and ongoing improvement, with a strong focus on customer experience.

Digital Experience and Engagement Team (DXE)

This team integrates communications, engagement, events, and human-centered design to improve how people experience UC IT services and to foster a more collaborative, people-focused digital culture.

From Foundation to Impact: The Office of the President's Next Chapter in AI Adoption

Scaling AI for Efficiency and Better Service

AI strengthened the Office of the President's operations by reducing manual work, improving response times, and enabling staff to focus on higher-value priorities. Building on last year's foundation, Technology Delivery Services (TDS) expanded AI adoption, fostered community through trainings and events, and delivered measurable efficiencies across key services. Ongoing training and communication continue to support responsible AI use at scale.

To sustain this progress, TDS strengthened the Office of the President's AI foundation through a roadmap, a return-on-investment-focused intake, and peer groups that support adoption. Communication, training, and collaboration will continue to guide responsible use and position us as a leader in practical, value-driven AI.

Building AI Skills Through ChatGPT and Microsoft Copilot Adoption

TDS launched ChatGPT and Copilot to help staff work more efficiently and build practical AI skills. More than 1,000 licenses have been deployed, and adoption continues to grow as teams incorporate AI into daily workflows. Engagement data shows that staff are using these tools consistently and in meaningful ways.

Foundation → Adoption → Impact

Office of the President AI by the Numbers

230K Prompts submitted since May 2025, reflecting sustained usage and growing capability

1000 Total AI licenses deployed:

- 700 ChatGPT
- 300 Copilot

800 Staff leveraged AI tools in their work from June–October 2025

200+ Participants at the AI Innovators Share Fair

Growing the Office of the President’s AI Knowledge and Community

UCOP Artificial Intelligence Hub

Embracing the Power of AI at UCOP

Artificial Intelligence (AI) is transforming the way we learn, solve problems, and drive innovation. At the University of California Office of the President (UCOP), we are committed to thoughtfully integrating AI into our operations to empower staff with the knowledge, tools, and confidence to use this technology effectively – while upholding the highest standards of safety, ethics, and responsibility.

The UCOP AI Hub: Resources for the UCOP Community

UCOP is dedicated to exploring the potential of AI to enhance our work and enrich

Vision

Our vision at the Univ
leader in the ethical a
transformative chang
AI solutions empowe
collaborative environ

Mission

At the University of C

Updating the AI Hub to Meet Staff Needs

Since launching in 2024, the AI Hub SharePoint site has become the Technology Delivery Services (TDS) central resource for AI guidance and training. In 2025, the TDS team refreshed the site to make it easier to navigate and more useful for everyday work. New resources include on-demand Copilot training and OpenAI training, project updates, AI tool common use cases, and clearer support materials for responsible use.

The AI Hub was designed to help staff adopt AI in meaningful and responsible ways. The site has had more than 2,000 total views since its launch, and its content continues to improve and evolve.

Collaboration and Learning: Deloitte Workshops

TDS partnered with the Deloitte GenAI Exploration Lab to strengthen leadership readiness for responsible AI adoption. The UC Operations leadership team, UC Investments, and UC Finance participated in dynamic AI workshops that explored the opportunities and risks of generative AI. These sessions provided practical insights into how AI can improve operations, inform decision-making, and support UC’s stewardship goals. Both events were highly successful, **drawing more than 165 attendees** and sparking meaningful conversations about innovation and responsible adoption.

The Power of Sharing: AI Innovators Share Fair

The AI Innovators Share Fair, sponsored by Academic Affairs and supported by a cross-functional planning team, gathered over 200 participants from across the Office of the President to explore real use cases demonstrating how AI can streamline work and support better service. Through live demos, early adopter lessons learned, and actionable guidance, participants gained a clearer understanding of how to apply AI responsibly and effectively in their own work.

Are you an Office of the President employee with ideas on how AI could improve workflows, solve problems, or spark innovation? Submit your thoughts!

Strengthening Operations With Practical AI and Automation

ESS Automation: A Game Changer for Operational Efficiency

The Technology Delivery Services (TDS) team, Enterprise Shared Services (ESS), manages system monitoring around the clock. Until recently, ESS staff had to manually address more than **80 system alerts**, which required overnight monitoring and significant time and attention.

In under three months, ESS leveraged AI and automation tools, including Copilot, ChatGPT, and Microsoft Power Automate, to streamline this work. The team automated **63 percent** of manual alert actions, reducing workload and generating an estimated **$60,000 in annual service cost savings.** ESS will continue refining this process to reduce repetitive tasks, support staff during high-demand periods, and strengthen overall operational resilience.

Improved Workflows by the Numbers

63% Of manual alert actions were automated, reducing workload

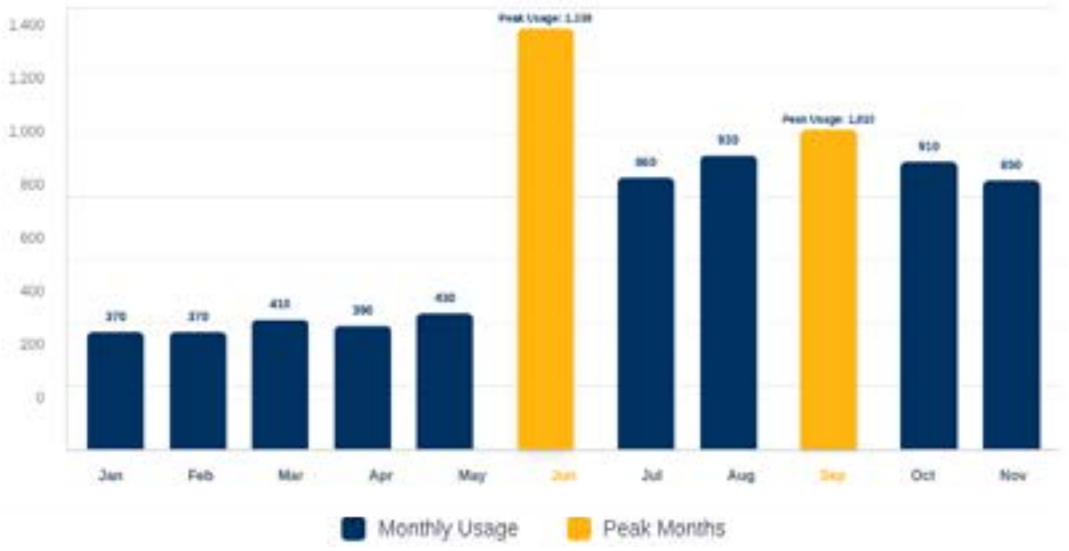
80 System alerts automated, no longer requiring manual monitoring

$60K Total estimated amount generated in annual service cost savings

Practical AI in Everyday Collaboration

Zoom AI Meeting Summaries Usage Grew Throughout 2025

Nearly 8,000 meeting summaries were generated in 2025.



Steady growth across 2025

8K	Zoom AI meeting summaries generated in 2025
1.3K	Peak usage during high-demand periods (June)
714	Average monthly Zoom AI summaries

Zoom AI Companion: Strengthening Collaboration Through Automated Summaries and Smarter Meeting Support

Technology Delivery Services (TDS) introduced Zoom AI Companion last year as part of its secure AI foundation. Adoption grew steadily, with roughly 250–300 staff members leveraging Zoom AI Companion features each month. Meeting summaries drove the highest engagement.

Adoption trends showed growing confidence in AI-assisted workflows and continued movement from foundational rollout to practical impact. TDS also planned live Zoom AI Companion training sessions for 2026 to provide guidance on the tool’s capabilities and data protection.

Improving Reliability and Stewardship Across the Office of the President's Technology Environment

San Diego Supercomputer Exit: Creating a Safer Technology Foundation for the Office of the President

This year, Technology Delivery Services completed a major behind-the-scenes upgrade that strengthened the technology foundation our teams relied on every day. The Office of the President retired all remaining systems housed at the San Diego Supercomputer Center (SDSC) and moved them into a modern cloud environment. While the work happened quietly in the background, the exit improved the stability and security of the systems that many teams relied on to do their work.

This transition allowed the Office of the President to clean up and modernize hundreds of aging systems and remove ~62,000 security vulnerabilities. By replacing outdated equipment and standardizing how systems are maintained, teams benefited from a safer, more stable environment that supports daily operations without interruption.

Reducing Risk Through Modernization

RETIRING LEGACY SERVERS AND MIGRATING SYSTEMS TO IMPROVE SECURITY AND STABILITY

389 Total SDSC Servers

204 Servers Migrated to AWS*

185 Decommissioned / Known Servers

10 Decommissioned / Unknown (zombie) Servers

~62,000 Vulnerabilities Eliminated

*14 migrated servers have active security exceptions

Why This Matters

Security vulnerabilities are weaknesses in systems that can be exploited to access information or disrupt services. By retiring outdated servers and moving to a modern cloud environment, the Office of the President eliminated significant vulnerabilities and lowered infrastructure costs. The reduction fortified the protection of sensitive UC data, lowered operational risk, and helped ensure that the systems our teams rely on every day remained stable and secure. It was a foundational improvement that supported better service and long-term reliability.

Operational Excellence Through Modernization and Stewardship

Modernizing Supplier Management Through a New Self-Service Portal

The Office of the President modernized supplier onboarding and maintenance by implementing a new supplier self-service portal. This capability replaced manual processes previously managed through email, Box folders, and standalone forms with a standardized, secure, system-driven model that allows suppliers to maintain their own information.

The new portal improved data accuracy, shortened turnaround times, and lowered fraud risk by ensuring banking and profile updates came directly from authenticated supplier accounts. It also enabled the Business Resource Center (BRC) and UC Finance teams to shift time from manual data entry to higher-value review and compliance activities.

Designed with future scalability in mind, the supplier portal established a reusable foundation that can support evolving UC requirements while improving day-to-day service delivery.

Strengthening Stewardship Through Financial System Contract Optimization

In a separate effort demonstrating Technology Delivery Service's leadership in financial stewardship, the team renegotiated UCOP’s Oracle financial system contract, reducing annual costs from $900K to $350K and securing $550K in ongoing yearly savings.

This optimization reflected Technology Delivery Service's broader commitment to operational excellence and resource efficiency, while ensuring that the Office of the President's financial systems remained both cost-effective and strategically aligned with the University’s needs.

Stewardship Impact

- Standardized, secure supplier self-service
- Reduced turnaround time and fraud risk
- Scalable foundation for future UC needs

> *“Our clients’ willingness to adapt and support system-driven change allows us to move away from long-standing manual processes toward more consistent, streamlined workflows. As we transition to the Oracle supplier portal, that partnership is essential to improving clarity and creating more efficient overall experiences.”*
>
> **BRC LEADERSHIP**

Designing and Delivering Services That Work for Everyone

IT Client Services: Service Excellence Grounded in Human Connection

IT Client Services (ITCS) remained one of the Office of the President's most trusted support teams, sustaining high levels of satisfaction and dependable service throughout 2025. Even during predictable surges, such as the post-curtailment return and the enterprise VPN transition, ITCS maintained strong responsiveness and consistent performance.

At the heart of this reliability was a simple philosophy: “behind every ticket is a person.” ITCS team members tailored support to individual needs, whether that meant a quick call, a walk-up conversation, or a clear self-service path. This intentional, people-first approach strengthened relationships and ensured customers felt supported, not just serviced.

This year, ITCS also expanded its use of AI to improve speed and create more capacity for high-value work. Staff used AI tools when appropriate to draft documentation and quickly summarize complex email threads. These efficiencies allowed the team to focus on deeper problem-solving and more personalized assistance.

Looking ahead, ITCS planned enhancements to knowledge resources, explored expanded self-service, and prepared new remote-support capabilities to meet customers where they are.

With stable operations, rising efficiency, and a commitment to thoughtful service, ITCS continued to set the standard for customer care at the Office of the President—proving that technology works best when it is guided by genuine human connection.

ITCS by the Numbers (2025)

88% Of calls answered, maintaining steady responsiveness (goal: 90%)

6:46 Average handle time, meeting the 5–7 minute service goal

☆☆☆☆☆☆

5.8 Out of 6, customer satisfaction score

> *“ITCS team members consistently make a strong, positive impression through collaboration and support. We always appreciate the team’s professionalism, approachability, and how easy it is to partner with them to get work done.”*
>
> **CUSTOMER VOICE**

Designing for Everyone: Improving Accessibility in UCPath

An estimated 20% of the general population has a disability that creates real barriers to using websites effectively.

With over 200K faculty and staff relying on UCPath for benefits and HR services, 20% could represent as many as 40K affected employees. In early 2025, the Technology Delivery Services Accessibility Team and UCPath, with support from UC location and the Office of the President stakeholders, began improving the UCPath self-service experience, with accessibility as a core priority.

One of the most significant efforts was making UCPath mobile-friendly for the first time—a major milestone for all UCPath customers, particularly those with disabilities who rely on mobile devices as their primary way to access online services. The accessibility team improved compliance with the Web Content Accessibility Guidelines 2.1 AA, enhanced screen reader compatibility for blind users, increased color contrast for those with low vision, and improved keyboard navigation for UCPath users without a mouse.

Accessibility enhancements and testing of UCPath reflected UC's commitment to equity and inclusion, empowering every employee to manage work and benefits independently.

Looking Ahead

As we look ahead, Digital Innovation & Technology remains focused on strengthening the foundations that enable the University's mission while adapting to a rapidly evolving technology landscape.

Our priorities center on protecting the institution, responsibly expanding capability, and delivering services that work well for the people who rely on them every day. Looking forward, we will prioritize:

- Enabling responsible use of AI to improve efficiency, insight, and decision-making.
- Advancing cybersecurity and digital risk to strengthen resilience across the UC system.
- Balancing strong stewardship with excellent customer servivce to ensure sustainable, high-quality IT services.

UNIVERSITY
OF
CALIFORNIA