

THE 14TH
CYBER
SECURITY
SUMMIT

UNIVERSITY
OF
CALIFORNIA

April 19, 2023
UCLA





Welcome

Dear Summit Attendees,

Welcome to the 14th Cyber Security Summit at the UCLA Carnesale Commons. This is our first in-person summit since we switched to a virtual conference format during the COVID-19 pandemic! We're so pleased to gather together to hear from cybersecurity thought leaders about topics affecting us today. We created the summit based on a foundation of sharing knowledge among information security professionals from across the University of California system, California State University, and the California Community Colleges.

This year, our experts are speaking about multiple topics related to cybersecurity, including two cyber legal case reviews, the law and the CISO, privacy-enhancing technologies, cross-industry insights for higher education, and how to create a security-first mindset. Our presenters come from a variety of cyber backgrounds, from the FBI to legal to the University of California system. By sharing information about these topics and discussing them with colleagues, we contribute to a collective mission of research, education, and public service. We hope the summit provides you with opportunities to see colleagues, develop new relationships, and have some fun along the way.

We hope you enjoy the summit back in person again!



The UC Cyber Security Summit Planning Team

Wendy, Jackie, Adrian, Ellen and Julie

Agenda

8:00 - 9:00 AM Check-in and Breakfast

9:00 - 9:15 AM Welcome

Van Williams Vice President of IT and Chief Information Officer, University of California
Jay Panchal Systemwide CISO, University of California

9:15 - 9:30 AM Activity

Jared Young Engagement Specialist, Go Team Events

9:30 - 10:15 AM US Government Cyber Case Studies: Lessons Learned

Olivia Olson Assistant Special Agent in Charge, Cyber & Counterintelligence Branch, FBI Los Angeles
Cameron Schroeder Chief, Cyber & Intellectual Property Crimes of United States Attorneys' Offices, DOJ Los Angeles
Discussion of two FBI cyber cases and their key take aways

10:15 - 10:30 AM Break and Activity

10:30 - 11:15 AM How to Develop a Security-First Mindset

Jenny Brinkley Director of Amazon Security
Learn how to design teams balancing culture, innovation and understanding of finite resources.

11:15 - 11:30 AM Break and Activity

11:30 AM - 12:15 PM Privacy Enhancing Technologies: From Theory to Practice

Dr. Rafail Ostrovsky Norman E. Friedmann Distinguished Professor of Computer Science and Mathematics, UCLA
Explore the benefits and adoption challenges of cryptographic techniques and applications.

12:15 - 1:45 PM Networking Lunch

1:45 - 2:00 PM Activity

Agenda

2:00 - 2:20 PM Optional Sponsor Listening Series with Fortinet

Leading Education cybersecurity for 2023 - 2025

2:20 - 2:40 PM Title: Optional Sponsor Listening Series with Mandiant

SOC Automation: Benefits and Proven Methods

2:40 - 3:00 PM Break and Activity

3:00 - 3:45 PM Law and the CISO

Sajjad Matin Principal Counsel for Cybersecurity and Data Protection in the UC Office of General Counsel
Franklin Monsour Jr Partner at Orrick, Herrington & Sutcliffe LLP
Review recent investigations and enforcement actions for potential legal liabilities facing information security officers.

3:45 - 4:00 PM Wrap-up

Monte Ratzlaff Systemwide Cyber Risk Program Director and UC Health Data Warehouse CISO, University of California

Speakers



OLIVIA OLSON

FBI, Los Angeles

Assistant Special Agent in Charge,
Cyber & Counterintelligence Branch

Olivia D. Olson is currently the Assistant Special Agent in Charge of the Cyber & Counterintelligence Branch in the FBI Los Angeles Field Office. ASAC Olson has dedicated her career to working counterintelligence and cyber matters. ASAC Olson served overseas as a Cyber Assistant Legal Attaché and in the Cyber Division at FBI Headquarters before reporting to the Los Angeles Field Office. ASAC Olson is currently responsible for Los Angeles Field Office squads covering Cyber, Counterintelligence, and Digital Forensics, as well as the Orange County Regional Computer Forensics Laboratory (RCFL).



CAMERON SCHROEDER

Department of Justice, Los Angeles

Chief, Cyber & Intellectual Property Crimes of
United States Attorneys' Offices

Cameron Schroeder is the Chief of the Cyber & Intellectual Property Crimes Section at the United States Attorney's Office in Los Angeles. Ms. Schroeder oversees a team of attorneys who prosecute federal crimes relating to computer and network intrusions and attacks, digital asset platforms, and IP infringement crimes, including trade secret theft/economic espionage. The Cyber & IP Section is housed within the National Security Division of the US Attorney's Office, reflecting its dual role of prosecuting crime and protecting the national security, and Ms. Schroeder and her team have a particular focus on nation-state cyber activities.

US Government Cyber Case Studies: Lessons Learned

Cyber crime comes in many forms, but with many common denominators, and this presentation will discuss two cyber intrusion cases: one dealing with ransomware in education and one with swatting-related intrusions committed by students. The briefing will discuss the vulnerabilities exploited in both cases, the special position that educational institutions occupy in the realm of cyber-crime, and lessons learned/best practices you can take to protect yourselves and your organizations.

Speakers



JENNY BRINKLEY

Amazon

Director of Amazon Security

Jenny Brinkley is the Director of Amazon Security, owning security awareness programs, upskilling strategies, and preparing for what's next in the security space. In her work, she partners with leaders both internally at Amazon and Amazon's top security-minded customers on how to implement security programs that scale and address the changing security climate considering geopolitical and technical advancements. Prior to joining Amazon, Jenny co-founded Harvest.ai, an artificial intelligence start-up focused on protecting highly sensitive data using behavior analytics to prevent data loss. Harvest.ai was acquired by AWS in April 2016. Jenny holds multiple data loss prevention patents, most interestingly one focused on the right to be forgotten from any digital environment.

How to Develop a Security-First Mindset

Understanding the role security plays in keeping the business safe while balancing a strong innovation culture, requires knowing how to prioritize teams and finite resources. In this session, learn how to intentionally design teams to deliver at scale while considering geopolitical risks, employee retention, and technology disruption.

Speakers



DR. RAFAIL OSTROVSKY

UCLA

Norman E. Friedmann Distinguished Professor of Computer Science and Mathematics

Dr. Rafail Ostrovsky holds Norman E. Friedmann Endowed Chair in Knowledge Sciences at UCLA Samueli School of Engineering and is a Distinguished Professor of Computer Science and Mathematics at UCLA. Prof. Ostrovsky joined UCLA in 2003 as a full tenured professor, coming from Bellcore where he was a Senior Research Scientist. Prior to beginning his career at Bellcore, he was an NSF Mathematical Sciences Postdoctoral Research Fellow at UC Berkeley. Dr. Ostrovsky received his Ph.D. in computer science from MIT in 1992. Prof. Ostrovsky is a Fellow of AAAS, ACM, IEEE, and IACR, and is also a foreign member of Academia Europaea. He has 15 U.S. patents issued and over 340 papers published in refereed journals and conferences. He is a member of the Editorial Boards of Journal of ACM, Algorithmica, and the Journal of Cryptology. He is the recipient of multiple awards and honors, including the 2022 W. Wallace McDowell Award, the highest award given by the IEEE Computer Society. At UCLA, Prof. Ostrovsky heads the Center of Information and Computation Security (CICS), a multi-disciplinary Research Center at UCLA Samueli School of Engineering. He is a co-founder of Stealth Software Technologies, Inc.

Privacy Enhancing Technologies: From Theory to Practice

Organizations that gather personal information for legitimate purposes are vulnerable to unauthorized entities accessing the information, which implies a responsibility to protect the information within each relationship. However, modern cryptographic tools allow organizations to secure the information they collect without sacrificing usability. By encrypting and distributing information between multiple computer systems within an organization, the risk associated with collecting and computing on sensitive information is minimized, even if one of the computers is lost, compromised, or stolen.

In certain policy contexts, organizations may need to analyze and search personally identifiable data across organizational boundaries for statutory, functional, or operational reasons. However, there are recognized risks and laws that discourage or forbid such exchanges, putting organizations at risk in trusting the parties they share data with. Advanced cryptographic techniques, such as “Secure Multi-Party Computation” and “Homomorphic Encryption,” allow for collaboration between two or more organizations or departments to extract actionable information without exchanging sensitive data, thereby avoiding non-compliance with regulations or litigation exposure.

This talk describes several success stories that illustrate the benefits of these and other cryptographic techniques and applications. Challenges to adoption will be touched upon along with opportunities for technology transfer.

Speakers



SAJJAD MATIN

UC Office of General Counsel

Principal Counsel for Cybersecurity and Data Protection

Sajjad Matin serves as the Principal Counsel for Cybersecurity and Data Protection in the UC Office of General Counsel. In his role, Sajjad counsels systemwide stakeholders through major cybersecurity incidents. Sajjad also serves as primary legal support to UCOP’s Office of Information Technology Services and Cybersecurity Audit Team, and advises UC Health, the Faculty Senate, and the UC campuses on a broad range of cybersecurity and technology matters.

Prior to his arrival at UC, Sajjad served as a federal prosecutor in Miami, Florida, where he focused on investigating and prosecuting cybercrimes, including intrusions and ransomware attacks. Sajjad’s experience also includes civil enforcement as an attorney with the Securities and Exchange Commission, where he investigated bribery, insider trading, and fraud against investors.

Prior to public service, Sajjad worked as an intellectual property attorney at Kirkland & Ellis LLP and later as in-house counsel for VMware, providing guidance on tech transactions and strategic partnerships.



FRANKLIN MONSOUR JR

Orrick, Herrington & Sutcliffe LLP

Partner

Franklin Monsour Jr is a white collar and investigations partner at Orrick, Herrington & Sutcliffe LLP, where he focuses his practice on defending life sciences and healthcare clients in government investigations and enforcement actions. He specializes in False Claims Act (FCA) and the Anti-Kickback Statute (AKS) cases, particularly those involving parallel civil and criminal allegations. Franklin previously served as a federal prosecutor in Miami, Florida, where he primarily handled civil enforcement, FCA, and criminal prosecutions in the healthcare and pharmacy industries. His cases included record-setting FCA recoveries and the largest compounding pharmacy healthcare fraud case to go to trial.

Law and the CISO

Presented by Sajjad Matin and Franklin Monsour Jr

Join two former federal prosecutors discuss their experiences on the intersection of law and technology. Sajjad Matin is Principal Counsel for Cybersecurity at UC OGC, and Franklin Monsour Jr. is a white collar and investigations Partner at Orrick, Herrington & Sutcliffe LLP. Sajjad and Franklin will explore the potential legal liabilities facing information security officers. This will include a review of recent civil and

UC Cyber Leadership



VAN WILLIAMS

University of California

Vice President of IT and Chief Information Officer

Van Williams is the Vice President of Information Technology Services and Chief Information Officer for the University of California, a \$40+ billion-dollar enterprise that spans ten campuses and six health care systems. As the UC CIO, Van serves as the university's chief IT leader and strategist, collaborating with campus and health CIOs, and other leaders across the UC system. Van also oversees IT related strategic priorities for the UC Office of the President (UCOP). Prior to UCOP, Van was the Vice Chancellor for Information Technology and Strategic Initiatives at UC Santa Cruz (UCSC) and served as the campus Cyber-Risk Responsible Executive. Van oversaw UCSC's \$800M technology organization and led a staff of 250. Before joining the UC system, Van spent more than 15 years at New York University in various senior roles, including Chief Information Officer for NYU's Stern School of Business. He has an MBA in finance, entrepreneurship and marketing from Stern, and a bachelor's degree from NYU, where he majored in classical civilization and minored in chemistry. Van is deeply committed to advancing diversity, equity, and inclusion initiatives and believes higher education is a key driver toward the creation of a healthy society.



JAY PANCHAL

University of California

Systemwide CISO

Jay Panchal is responsible for ensuring cybersecurity throughout the UC system by collaboratively developing and implementing a university-wide information security program and coordinating its operations across all UC locations. He advises the UC Board of Regents, senior executives and senior management, and President Drake and chancellors on security compliance, cyber risk, incident management and cyber resilience. Panchal also represents UC on international and national cybersecurity initiatives and organizations, serving as a thought leader, engaging with colleagues nationwide and participating in conferences and other forums.

Prior to UC, Jay served as global chief information security officer at the International Monetary Fund (IMF) since 2009. During his tenure at the IMF, Panchal led all aspects of information security and cyber risk management to enable the IMF to achieve its goals, safeguard its reputation and operations, and protect its assets globally. In addition, he represented the IMF at United Nations' cybersecurity functions and led a multi-year cyber-risk-awareness program that resulted in a 90% risk reduction in susceptibility to the IMF's highest-risk threats and received a CIO Excellence Award. Prior to the IMF, Panchal served as a global Information Security Risk manager at Barclays and provided governance and oversight for e-commerce and security at Deutsche Bank.

Performer



JARED YOUNG

Go Team Events

Engagement Specialist

Jared Young is known as an engagement specialist because he turns gatherings into experiences. He builds connection and community, helping participants see the true value in relationships. Jared has served as an MC/Host at hundreds of events for companies globally including Google, Netflix, Nestle, American Airlines, Home Depot, Exxon Mobil, and more. While every crowd is different, Jared's energetic personality ensures that everyone feels welcome at your event.

Recent hosting highlights include hosting a Top Chef live showdown event with Top Chef finalist Shirley Chung and Eric Adjepong; appearing alongside several past American Idol finalists and America's Got Talent host Howie Mandel at NBC's annual St. Joseph Hospital fundraiser at Universal Studios; hosting a President's Club for a major medical device company for 800+ attendees in Cabo San Lucas alongside NFL Legend Jerry Rice; hosting a recent St. Jude event with baseball legend Cal Ripken Jr, and MC'ing an amazing virtual event with Darryl Hall, Sheryl Crow, and Jewel.

Event Moderator



MONTE RATZLAFF

University of California

Systemwide Cyber Risk Program Director and UC Health Data Warehouse CISO

Monte Ratzlaff is the systemwide Cyber Risk Program Director and UC Health Data Warehouse CISO at the University of California Office of the President where he works with UC leaders to establish cyber risk strategic plans and objectives. He also leads the UC Health Chief Information Security Officers from each location in various information security-related initiatives. In his prior role at UC Davis Health System, Ratzlaff managed the IT Security department and served as the Chief Security Officer. He has extensive experience in information security within the banking and health care industries and holds Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) professional designations. As a cybersecurity leader with over 23 years of experience, he has been a speaker at numerous events.

Platinum Sponsor Speakers

BOB TURNER

Fortinet
Field CISO for Education

Leading Education Cybersecurity for 2023 – 2025

If you thought the past three years were rough on Education CISOs, you'll want to hang on tight as the challenges of cybersecurity leadership in higher education continue to drive change over the next two years. From AI to ZTNA, this short presentation will include four things the Education CISO will need to emerge victorious over emerging challenges of maintaining talent in the face of dwindling talent pools, continually increasing cybercrime, and operational disruptions.

BRIAN YOUNG

Mandiant
Security Customer Engineer

SOC Automation: Benefits and Proven Methods

The needs of automation in a modern SOC are paramount when considering availability of skilled security analysts are at a premium and that threat actors are increasingly using more automation themselves. Utilizing a Security Orchestration Automation and Response (SOAR) solution to automate the noise and frequent risks enables the SOC to focus on more important activities. In addition, we will share how routinely testing the entire system of detection and prevention assists a SOC by automating the question of "are we at risk for x" so the team can close gaps, which is also critical for a modern security posture. Join us as we explore the benefits and proven methods of these SOC Automation solutions to learn more.

Sponsors

Thank you to our 2023 Cyber Security Summit Sponsors!

PLATINUM

MANDIANT

Trellix

FORTINET

GOLD

CROWDSTRIKE

Abnormal

netskope

AHEAD

CDW
Education

paloalto
NETWORKS

SILVER

DELL Technologies

SailPoint

zscaler

PUBLIC SECTOR

UC Exhibitor

UC IT BLOG

The UC IT blog is by, for, and about everyone working in IT across the UC system. Representatives joined the UC Cyber Security Summit Expo Hall, where they shared information about how to feature and share the expertise of our community.

CYBER SECURITY SUMMIT



The University of California Cyber-Risk Coordination Center (C3) has already begun planning the 15th Cyber Security Summit. Keep up-to-date on our website at security.ucop.edu/get-involved/uc-cybersecurity-summit.

We welcome your suggestions about possible topics and speakers. Please contact uccybersummit@ucop.edu.



UC CYBER-RISK COORDINATION CENTER
Fostering collaboration between cybersecurity professionals for a stronger and more secure UC