

The 6th Biannual

# CYBER SECURITY SUMMIT

October 24, 2018  
UC Riverside

UNIVERSITY  
OF  
CALIFORNIA



# AGENDA

8:00-9:00 AM

**Breakfast & Check-in**

9:00-9:15 AM

**Welcome**

**DAVID RUSTING, SYSTEMWIDE CHIEF INFORMATION SECURITY OFFICER, UCOP**

9:15-9:30 AM

**Icebreaker: What Do You Want?**

**CHRIS KNIERIM, LEADERSHIP CONSULTANT, STAND UP SUCCESS**

What would you like to see from UC in terms of cyber leadership? Defining what you want is the first step in getting what you want. Did you come to this summit with expectations for UC in terms of cyber leadership? In this powerful activity, you will define and share what you want with some of your peers. Setting a specific target is one of the pillars of being effective, efficient, and successful in anything you do.

9:30-10:15 AM

**Keynote: Improving Cybersecurity through a Diverse Workforce**

**CAMILLE CRITTENDEN, DEPUTY DIRECTOR, CITRIS AND THE BANATAO INSTITUTE**

Like many institutions, the University of California faces a growing demand to strengthen its cyber infrastructure over the next 10 years, including increasing the number of roles in cybersecurity. The University is in a unique position to serve its missions in education, research, and public service through measures to respond to this challenge. Creating a more diverse workforce—in terms of gender, race and ethnicity, economic background, and other parameters—throughout the ranks of cybersecurity professionals, will create a more robust environment to protect vital business applications, research data, and personal information. Dr. Crittenden's talk will explore the current demographics in academic information technology and cybersecurity more broadly, and suggest measures to improve diversity metrics and expand opportunities throughout the organization.

10:15-10:30 AM

**Break**

10:30-11:15 AM

**Fannie Mae's DevSecOps Journey**

**STEPHANIE DERDOURI, DIRECTOR OF VULNERABILITY MANAGEMENT AND INFORMATION SECURITY, FANNIE MAE**

Fannie Mae partners with lenders to create housing opportunities for families across the country, and helps make affordable rental housing and the 30-year fixed-rate mortgage possible for millions of Americans. To support this mission, Fannie Mae must encourage robust security practices throughout the organization. For years, Fannie Mae has aimed toward: 1) conducting cybersecurity assessments earlier in the development lifecycle; and 2) engaging business partners in the review and mitigation of cybersecurity risks. Through DevSecOps, Fannie Mae has now reached that goal, and stakeholders from development, operations, and cybersecurity now monitor, analyze, test, and proactively determine and fix vulnerabilities earlier in the development lifecycle. Join us for this session to see how DevSecOps has helped to dramatically increase code quality standards and reduce vulnerabilities at Fannie Mae.

**All summit sessions will be held in the UC Riverside Highlander Union Building (HUB), room 302.**

11:15-12:00 PM

**Cyber Risk Transfer: Cyber Insurance as a Critical Component of Cyber Risk Management for Large Institutions**

**LAUREN CISCO, SENIOR VP OF THE CYBER CENTER OF EXCELLENCE, MARSH  
MARTIN LEICHT, ASSISTANT VP OF THE CYBER CENTER OF EXCELLENCE, MARSH**

As individuals and organizations become more reliant on data and technology every day, the threat of security or privacy (“cyber”) risk events continues to evolve and escalate. With growing risk, cyber insurance has become an increasingly relevant and important component of organizations’ plans for cyber risk management. UC’s cyber insurance broker, Marsh, will be highlighting the evolution of cyber insurance, the current state of the marketplace, and how it is helping organizations, specifically those in higher education, assess, transfer, and respond to cyber risk.

12:00-1:30 PM

**Networking Lunch**

1:30-2:00 PM

**Engagement Activity: Take Action and Take Responsibility**

**CHRIS KNIERIM, LEADERSHIP CONSULTANT, STAND UP SUCCESS**

In the first icebreaker activity we posed the question, “What would you like to see from UC in terms of cyber leadership?” We now ask, “What action would you take to make that happen?” Leaders take action and they take responsibility to make things happen. In this powerful, interactive, and fun activity, we’re going to explore the actions you can take to improve cyber leadership and then share those actions with your peers to understand different perspectives.

2:00-2:45 PM

**Chaos to Control**

**HENRY DUONG, INFRASTRUCTURE SECURITY MANAGER  
EDWIN HART, ENTERPRISE SECURITY ARCHITECT  
UNIVERSITY OF KANSAS HEALTH SYSTEM**

While some believe that the healthcare industry might have more protection due to regulations, this is often not the case. Henry Doung and Edwin Hart discovered the need for an overhaul of the University of Kansas (KU) Health System when they arrived there as information security professionals. Their first hard data point showed that thousands of malware infections plagued the system. Moreover, the system lacked visibility and needed better staffing. Doung describes their time at KU as a movement from chaos to control. In their talk, Doung and Hart detail their successful 3-year journey to create a secure system and a culture that promotes proactive threat mitigation and successful cybersecurity management.

2:45-3:00 PM

**Break**

3:00-3:45 PM

**Cybersecurity for the State of California: One Team, One Fight**

**PETER LIEBERT, CISO, CALIFORNIA DEPARTMENT OF TECHNOLOGY**

Think the private sector has issues securing its data? Try securing an entire state! Peter Liebert will give a quick primer on the complexities of California’s IT resources, its governance structure, and the traditional challenges that the state faces. He will then outline the state’s Vision 2020 concept and the “one team, one fight” strategy that his office and its four core strategic partners are using to tackle these challenges.

3:45-4:00 PM

**Wrap-up**

**DAVID RUSTING, SYSTEMWIDE CHIEF INFORMATION SECURITY OFFICER, UCOP**

## SPEAKERS



### Camille Crittenden

**DEPUTY DIRECTOR, CITRIS AND THE BANATAO INSTITUTE**

Dr. Camille Crittenden serves as Deputy Director of CITRIS and the Banatao Institute, Director of the CITRIS Connected Communities Initiative, and Co-Founder of the Women in Technology Initiative at the University of California. Prior to coming to CITRIS in 2012, she was Executive Director of the Human Rights Center at Berkeley Law, where she helped develop its program in human rights, technology, and new media. Dr. Crittenden has written and spoken widely on these topics, as well as on technology applications for civic engagement, government transparency and accountability, and the digital divide. She held previous positions as Assistant Dean for Development with International and Area Studies at UC Berkeley and in development and public relations at the University of California Press and San Francisco Opera. She earned an M.A. and Ph.D. from Duke University.



### Stephanie Derdouri

**DIRECTOR OF VULNERABILITY MANAGEMENT AND INFORMATION SECURITY, FANNIE MAE**

Stephanie Derdouri operates as Fannie Mae's Director of Vulnerability Management, ensuring the organization is protected against information security vulnerabilities that could jeopardize its mission of providing support to homebuyers. Derdouri oversees Fannie Mae's Application Security (AppSec) and the Vulnerability Threat Management (VTM) teams that perform application security assessments and vulnerability scanning, and that facilitate network penetration and data exfiltration testing. Previously, Stephanie worked for a.i. Solutions and led the NASA Headquarters Risk Management and Federal Compliance Team to develop and apply strategies to manage cybersecurity risks. She has also worked as a Security Analyst for the U.S. Department of Justice, where she honed and exercised her expertise in information security and vulnerability management. Derdouri earned a B.S. in Computer Science from The George Washington University and an M.S. in Information Systems Engineering from Johns Hopkins University.



### Martin Leicht

**ASSISTANT VICE PRESIDENT OF THE CYBER CENTER OF EXCELLENCE, MARSH**

Martin (Marty) Leicht is a member of Marsh's National Errors and Omissions (E&O), Cyber Center of Excellence, and focuses on placements of professional liability and cyber insurance coverages for large U.S. commercial accounts. Marty is responsible for identifying and negotiating complex risk transfer solutions with insurance carriers to help clients address professional liability and cyber exposures. Marty also leads the Cyber Center of Excellence's industry working groups for the Higher Education and Hospitality sectors. Prior to joining the E&O, Cyber Center of Excellence, Marty was a full-time associate in Marsh's New York Metro Financial and Professional Products (FINPRO) Advisory Group, supporting the team in the placements of directors and officers liability, fiduciary liability, employment practices liability, and commercial crime insurance coverages. Prior to joining FINPRO as a full-time associate, Marty spent time in Marsh's Global Energy Practice and in Marsh's Boston National Brokerage group.



### Lauren Cisco

**SENIOR VICE PRESIDENT OF THE CYBER CENTER OF EXCELLENCE, MARSH**

Lauren Cisco joined Marsh in 2017 and is a Senior Client Advisor in Marsh's Cyber Center of Excellence. She provides guidance and support to complex accounts on topics related to cyber technology risks. She specializes in risk transfer strategy, and implementation for Cyber, Technology Errors & Omissions (E&O), Professional Liability, and Media Liability coverage. Prior to joining Marsh, Lauren was a Cyber and E&O specialist at JLT Specialty USA. During her time with JLT, she spent two years in London, working with retail and wholesale clients around the world on coverage for cyber, content, and technology risks. She began her insurance career with Aon in 2005, working initially in Account Management before transitioning to Cyber and E&O brokerage in 2010.

## SPEAKERS



### Chris Knierim

#### LEADERSHIP CONSULTANT, STAND UP SUCCESS

Chris Knierim is an award-winning international corporate trainer, speaker and comedian who has the unique ability to create effective, entertaining, and engaging learning experiences. Chris leverages his recognized Leadership and Quality Systems Implementation experience gained from working with multiple organizations, from fortune 50 companies to start-ups, in the highly regulated industry of medical devices and life science. Chris empowers you to realize your vision for yourself, your team, and your culture in a fun and impactful way. He provides proven values-based strategies that increase efficiency and effectiveness, leading to more client profitability.



### Henry Doung

#### INFRASTRUCTURE SECURITY MANAGER, UNIVERSITY OF KANSAS HEALTH SYSTEM

Henry Doung is the Infrastructure Security Manager at the University of Kansas (KU) Health System. He specializes in developing cybersecurity strategies and building metrics and other tools to enhance organizational communication related to cyber risks, threats, and attacks. Prior to coming to KU, Henry served as a network engineer at State Street Bank and was in charge of cybersecurity at the law firm of Shook, Hardy, and Bacon. In addition to his degree in Computer Information Systems, Henry is a certified ethical hacker and a certified penetration tester.



### Edwin Hart

#### ENTERPRISE SECURITY ARCHITECT, UNIVERSITY OF KANSAS HEALTH SYSTEM

Edwin Hart, an IT and Security Professional with over two decades of experience, is an Enterprise Security Architect at the University of Kansas Health System. He has held positions in multiple IT fields, including network, systems, operations, quality assurance, database, and security. Information security is of the utmost importance in many areas, and this is especially true for the healthcare industry. At KU, Edwin uses his wide-ranging skills to consider multiple perspectives, pushing traditional security boundaries and utilizing cutting edge database and profiling techniques. A common demand for user mobility and flexibility also requires a strategic approach to security. Edwin responds to this need by embracing early-stage technologies entering the infrastructure while also accepting early-stage countermeasures. He finds that this approach allows KU to detect attacks that, as technology evolves, leave more and more subtle indications of their presence. Along with Henry Duong, Edwin will be discussing KU Health System's transformational path to an effectively secured environment.



### Peter Liebert

#### CHIEF INFORMATION SECURITY OFFICER OF THE CALIFORNIA DEPARTMENT OF TECHNOLOGY

Governor Jerry Brown appointed Peter Liebert as Chief Information Security Officer (CISO) and Director of the Office of Information Security of the California Department of Technology (CDT) on November 14, 2016. Mr. Liebert is the primary state government authority (as defined by California Law AB 670) charged with ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information assets. He is involved in a broad range of activities within the state and collaborates with federal, state, and local security professionals, higher education organizations, private industries, and others on security related matters. Mr. Liebert is responsible for creating, issuing, and maintaining standards, procedures, and policies related to all aspects of information security for the state. He is committed to securing the state's information assets by providing statewide leadership and collaboration and recently received the "State Cybersecurity Leader 2017" award from StateScoop.

## SPONSORS

Thank you to our Fall 2018 Cyber Security Summit Sponsors!

