SPRING CONFERENCE

CYBER IN ACTION

April 10-12, 2017

Hilton Los Angeles/Universal City
California, USA

CSX™
CYBERSECURITY NEXUS

ISACA®
Trust in, and value from, information systems
Los Angeles Chapter

Connecting Women Leaders in Technology
ENGAGE. EMPOWER. ELEVATE.
ISACA

On behalf of the Los Angeles Chapter of ISACA (ISACA-LA) we want to welcome you to our 2017 Spring Conference, "Cyber in Action," a theme developed in support of ISACA International's Cybersecurity Nexus initiative (www.isaca.org/cyber). We have come a long way since our now International organization was first formed in Los Angeles in 1967, when a small group of auditing professionals whose jobs were to audit controls in computer systems, sat down to discuss the need for a centralized source of information and guidance in the field. We will be celebrating our 50th anniversary in 2 years with various celebratory events along with a joint conference with ISACA International instead of our annual Spring Conference. We are proud of our diverse membership today, which includes a variety of professional IT-related positions—to name just a few, IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor. Some of us are new to the field, others are at middle management levels and still others are in the most senior ranks. We work in nearly all industry categories, including financial and banking, public accounting, government and the public sector, utilities and manufacturing. Our Spring Conference 2017 gives good reason for our diverse group to come together - to learn, to fulfill our IT governance and cybersecurity responsibilities and to better deliver value to the business. We hope you will join us in what promises to be an energizing and worthwhile Spring Conference 2017!

Nelson Gibbs
President, ISACA Los Angeles Chapter

Debbie A. Lew
Chair, Spring Conference 2017

Conference Committee

Debbie Lew – Chair
Ernst and Young, LLP

David Alexander – Sponsors & Vendors
Los Angeles Department of Water and Power

Sylvia Barnes – Student Volunteer
Los Angeles Southwest College

Michael Bobrowicz – Audio Visual
Net Force

Joshua Chin – Audio Visual
Net Force

Larry Hanson – Communications & Registration
MUFG Union Bank

Prasad Kodukulla – Marketing and Social Media
City of Hope

Karen Norton – Sponsors & Vendors Project Manager
DirecTV (ATT)

Cheryl Santor – Vice Chair, Sponsors and Vendors
Metropolitan Water District of Southern California, Retired

Mike O. Villegas – Sponsors & Vendor
K3DES LLC

Don Almario – Sponsors & Vendors
Los Angeles Insurance Company

Jonathan Chan – Conference Webmaster
Deloitte & Touche

Min Fu – Conference Project Manager
Ernst & Young, LLP

Lisa Kinyon – Facilities
Bank of America

Kelly Lin – Registration
KPMG

Thomas Phelps IV – Program, Sponsors & Vendors
Laserfiche

CYBER IN ACTION

The ISACA Los Angeles Chapter's conference provides a unique opportunity for IT assurance, security, risk management and governance professionals to explore cybersecurity topics with knowledgeable experts, expand professional skills and enhance career potential.

Leverage the benefits of a powerful learning experience with the value of the ISACA Los Angeles Chapter's Conference:

- Sharpen your skills with practical and relevant sessions that apply to your current or prospective roles and responsibilities.
- Tailor a learning experience that fits your style, budget and professional goals.
- Revisit with old friends, make new friends and network throughout the conference including the networking reception on Monday night.
- If you're an IT Audit Director, be invited to our IT Audit Directors' Forum to network and discuss emerging IT audit issues and risks.
- Learn about technology solutions at the Vendor Exhibition Fair that can address the challenges you face in your current role.
- Earn up to 20 CPE credits, to help you become or remain certified.
- Attend the CSX Cybersecurity fundamentals workshop to prepare for the cybersecurity fundamentals exam.

Learn from experienced Cybersecurity leaders

The ISACA Los Angeles Chapter has brought together leading IT governance, risk, security and assurance leaders to share their experience and knowledge with you. They live the topics they teach, and draw from a deep understanding of the complex issues facing IT professionals today. This real world perspective means that attendees benefit from proven solutions and best practices.

Location and dates

April 10th – April 12th, 2017

Hilton Los Angeles/Universal City,
California USA

Registration

Register online at www.isacala.org/conference.

Payment can be made by credit card, check or wire transfer

NOTE: Registration will not guarantee acceptance into a session until the payment is also received. PAYMENT must be postmarked by the early registration date (March 27, 2017) in order to qualify for the Early Registration discount.

Conference Fees	1 Day	2 Days	3 Days
	Pre-conference Workshop	Pre-conference Workshop	Full Conference (Mon. – Wed.)
ISACA/ISSA/IIA Members	$200	$400	$650 ($750 after March 27)
Non Members	$250	$500	$750 ($850 after March 27)
Full Time Students	$100	$150	$250 ($300 after March 27)

Monday April 10

Keynote Session

The Game is Changing and How do We?

Keynote Speaker

James Rinaldi

Chief Information Officer, NASA Jet Propulsion Laboratory (JPL)

When it comes to executing on mission critical programs, failure is not an option—especially when it involves robotics and space exploration. Whether it's landing NASA's Curiosity rover on Mars—with millions of people watching a live stream—or launching the WFIRST telescope in 2020 to explore dark energy, Jet Propulsion Laboratory (JPL) technology developed for NASA's missions also benefits lives on Earth.

When the world is watching, information security becomes a critical component in NASA JPL missions. This keynote from Jim Rinaldi, CIO of JPL, will provide an overview of how JPL's technology innovation is seen in everything from today's autonomous vehicles to how Amazon implements Cloud for federal programs. Jim will provide an overview of JPL's cybersecurity strategy, the importance of audit, and what the future looks like with advanced analytics capabilities. The CIO will describe how the world is changing and what JPL, and other leading organizations, need from their cybersecurity programs to keep up with rapid advancements in technology.

About James Rinaldi

James Rinaldi is NASA Jet Propulsion Laboratory's (JPL) Chief Information Officer and Director for Information Technology. He has management responsibility for JPL's Information Technology Directorate. His responsibilities include developing and executing IT strategies, architecture and planning that align with the needs of JPL. Cybersecurity strategy, planning and execution are a top priority for the CIO.

James is a member of the JPL Executive Council and participates in the Lab's governance councils. He also participates in NASA's IT governance council and represents JPL's IT at NASA IT meetings.

James has more than 30 years of experience with information systems in government and industry. He was the Chief Information Officer at the U.S. Food and Drug Administration where he had overall responsibility for the planning, development and delivery of information systems across the FDA. Prior to that, he was the Chief of Information Technology Services at the IRS and Chief of Business Systems Integration. While at the IRS, James helped develop the Free Tax Alliance e-Gov initiative as well as provide guidance and expertise on the IRS Modernization efforts. James spent 16 years at the Marriott Corporation in Bethesda, MD, where his last position was senior vice president for information resources, operations and services. He was responsible for designing, building and operating Marriott International's technology infrastructure, consisting of computer hardware, software and global networking for over 2,000 locations, including the corporate computing center. He was directly involved in Marriott's E-commerce business, business processes and initiatives, as well as Web architecture hosting. James has a bachelor of arts in computer science from the University of North Florida in Jacksonville. He has successfully completed executive and leadership development programs at the University of Maryland in College Park.

Keynote Panel

Women in Technology: Facing Today's Challenges While Building Tomorrow's Workforce

Join us for a panel discussion on Women in Technology and hear from some of the most influential women technology leaders from non-profit; private industry; and federal, state, and local government. It's sure to be an engaging dialogue as they discuss their paths to leadership in a male-dominated industry, their thoughts on emerging cyber risks, their experiences in attracting and retaining top IT talent in a competitive market, and the lessons they've learned along the way.

Moderator

Theresa Grafenstine

Inspector General, U.S. House of Representative

In 2010, the Honorable Theresa M. Grafenstine was named the Inspector General of the U.S. House of Representatives, having been unanimously appointed by the House Speaker, Majority Leader, and Minority Leader. She has served for twenty-five years in the Inspector General community in both the legislative and executive branches of the US Government. She is also an active volunteer in support of the information technology, governance, internal auditing, and accounting professions.

Ms. Grafenstine currently serves on the board of directors of the Association of International Certified Professional Accountants (AICPA). With over 650,000 members, the AICPA is the world's largest member association representing the accounting profession. Ms. Grafenstine is also the Vice-Chairman of the international board of directors of ISACA, a global association with over 140,000 members in the IT audit, governance, security and risk profession. She also provides financial oversight as the audit committee chairman of the Pentagon Federal Credit Union, which has over $21 billion in assets and 1.3 million members.

Panelist

Gina L. Osborn

Assistant Special Agent in Charge of the Cyber and Computer Forensics Programs, FBI

Ms. Osborn began her law enforcement career in 1986 by enlisting in the U.S. Army as a Counterintelligence Special Agent. She spent six years in Belgium and Germany during the Cold War working the highest profile espionage cases in the European Theater. During Operation Desert Storm,.

In 1996, Ms. Osborn became a Special Agent with the Federal Bureau of Investigation. She was assigned to the Los Angeles Field Office with duty in the Santa Ana Resident Agency.

Ms. Osborn worked on a task force with detectives from the Westminster Police Department to investigate Asian Organized Crime in the Little Saigon District of Orange County, California. As a result of her efforts, several Asian Criminal Enterprises involved in violent crimes including extortion, loan sharking, drug trafficking and murder for hire were disrupted and dismantled.

On September 11, 2001, Ms. Osborn was reassigned to work on international terrorism matters. In 2003, she was promoted to the position of Counterterrorism Program Coordinator for the Los Angeles Division of the FBI. She later supervised the

Extraterritorial Squad which was responsible for conducting terrorism investigations against U.S. persons and U.S. interests in Asia, India and Australia.

Ms. Osborn was promoted to Assistant Inspector, Team Leader, in the Inspection Division at FBI Headquarters. She led teams in the review and assessment of investigative programs in field offices and Headquarters' entities. Ms. Osborn specialized in inspecting International Terrorism and Cyber Programs and collaborated with the Cyber Division at FBI Headquarters to improve operations nationwide.

In 2007, Ms. Osborn returned to Los Angeles as the Assistant Special Agent in Charge of the Cyber and Computer Forensics Programs for the Central District of California. She currently oversees investigations relating to national security and criminal computer intrusions. Additionally, Ms. Osborn provided foundational leadership in the creation of the Orange County Regional Computer Forensics Lab (OCRCFL). The OCRCFL is part of a national network of FBI-sponsored, full-service forensics laboratories and training centers devoted entirely to the examination of digital evidence in support of federal, state, and local criminal and terrorism investigations.

A native of Orange County, California, Ms. Osborn received her Bachelor of Science degree in Psychology from the University of Maryland.

Panelist

Jeanne Holm

Deputy CIO, Assistant General Manager, and Senior Technology Advisor, City of Los Angeles

As a leader in open data, education, community-building, and civic innovation, Jeanne Holm empowers people to discover new knowledge and collaborate to improve life on Earth and beyond. From citizens of Los Angeles to astronauts in space to rural villagers in Uganda, billions of people have used her systems to find the data, information, and knowledge they need to make better decisions every day.

Jeanne is the Deputy CIO, Assistant General Manager, and Senior Technology Advisor to the Mayor for the City of Los Angeles, bringing technical innovations to 4 million people. She oversees technology planning and strategies for the City as well as customer engagement for technology internally and with the public addressing issues from climate change to homelessness to improving city services. As the former Evangelist for Data.Gov (an open government flagship project for the White House), Jeanne led collaboration and built communities with the public, educators, developers, and governments in using open government data. She has been a senior consultant with the World Bank, where she empowers governments and civil society to use open data to increase prosperity and civic good. She was the Chief Knowledge Architect at NASA's Jet Propulsion Laboratory at the California Institute of Technology, where she drove innovation through collaborative systems, knowledge sharing, and social platforms. She architected systems and managed teams from the award-winning NASA public portal to pioneering knowledge architectures within the U.S. Department of Defense. She is a Distinguished Instructor at UCLA, teaching courses in knowledge management, big data, and civic innovation. She is the CIO and Director for Education for In Unison, a charity that promotes peace and social justice through education and music. She is a Fellow of the United Nations International Academy of Astronautics, co-Chair of the Africa Open Data community, and has more than 130 publications on innovation, open data, information systems, and knowledge management.

Panelist

Jessica Bair

Senior Manager, Advanced Threat Solutions, CISCO

Jessica Bair is a Senior Manager, Advanced Threat Solutions at Cisco Security, where she manages alliance partnerships for the AMP Threat Grid unified malware analysis and threat intelligence platform. Prior to the acquisition by Cisco, Jessica was Senior Director of Business Development at ThreatGRID. Jessica was at Guidance Software for thirteen years; including VP of Professional Services, and co-creating the EnCase Certified Examiner (EnCE) certification in 2001 and creating the EnCase Certified eDiscovery Practitioner (EnCEP) program in 2009. Prior to Guidance Software, Jessica served several years as a special agent/computer forensic examiner in the U.S. Army Criminal Investigation Command. She earned a MBA in Strategic Planning from Pepperdine University, Malibu, CA.

Panelist

Andrea Hoy

CEO, A. Hoy and Associates and President of Information Systems Security Association (ISSA)

Andrea received her initiation into the information security community when her hard work and dedication earned her the role of Assistant Venue Manager/Supervisor at the 1984 Summer Olympics in Los Angeles, California. This position exposed her to the information security field and ignited a passion that has made Andrea, arguably, one of the leading women in her profession. She has not only served as an advisor to the Pentagon, but in 1991 Andrea received the Security Education Manager's Award, presented to her by a representative from the Pentagon, acknowledging her work in applying Continuous Process Improvements to the implementation of information security resulting in cost savings for both industry and Government. She has been involved in numerous committees in Washington, D.C., to establish national and international information security policies. She has assisted companies in establishing policies and procedures that comply with international privacy laws such as the European Union Privacy Directive, the Data Protection Act of 1998, and the Wet Bescherming Persoonsgegevens (WBP) Dutch Personal Data Protection Act of 2000, as well as U.S. privacy regulations such as the Gramm Leach Bliley Act 1999(GLBA), a.k.a. the Financial Modernization Act, the Health Insurance Portability and Accountability Act 1996 (HIPAA), PCI, as well as internationally accepted standards such as ISO17799/27001 & 27002.

Andrea is CEO of A. Hoy & Associates, and has recently founded Sense1 Security, Inc., a thriving information security consulting firm that was established to provide essential information security expertise on immediate and specific information security and business continuity planning. The services provided range from a quick policy review to wireless vulnerability risk assessments, cyberforensics/ investigations, senior management briefings, quantifiable IT and privacy risk assessments, business continuity/disaster recovery planning and assisting with developing a total information security strategic plan customized to the specific company culture quickly and efficiently with the utmost discretion.

Andrea has served as the Chief Technical Officer of iQwest Technologies, focusing on security and compliance initiatives with CISOs from various Siemens operating companies and other leading global businesses.

She can often be found doing what she is most passionate about which is speaking engagements throughout the nation to promote awareness of vulnerabilities and trends in the IT security field. She has been consulted by various media outlets and conferences with speaking engagements and interviews on cutting edge security and compliance issues. Andrea's commitment to education has driven her to create a nationwide "Chief Information Security Officer (CISO) Bootcamp," which addresses best practices of security management.

Tuesday April 11

General Session

The State of Cybersecurity

Jessica Bair

Senior Manager, Advanced Threat Solutions, CISCO

The Cybersecurity industry is undergoing a major transformation. Hackers have industrialized and their attacks continue to grow in sophistication. These attackers are organized, well-funded and very motivated; typically nation-states or organized criminals.

We are in a Cybersecurity arms race. To have effective Cybersecurity, we must build an architecture that is:

- Simple to use, as the demand for number of qualified Cybersecurity professionals continues to outstrip the human resources
- Open to all technologies, from the largest vendors to the newest start-ups
- Automated, not only reduce the time from breach to detection, but also to compensate for the severe shortage of skilled staff

Conference Schedule

Pre-Conference Workshops (Limited Seating)

APRIL 8 - SATURDAY

08:30 to 05:00	WS1	**CSX Cybersecurity Fundamentals (Day 1)** **Mike O. Villegas,** Vice President, K3DES LLC
	WS2	**Web Application Security for Dummies (Hands on Workshop Day 1)** **Lee Neely,** Senior Cyber Analyst, Lawrence Livermore Laboratory, **Chelle Clements**, Senior Cyber Analyst, Lawrence Livermore Laboratory, **Jim McMurry,** CEO, Milton Security
	WS3	**Malware Analysis for Non-Programmers (Hands on workshop - Day 1)** **Peter Morin,** Principal Cyber Engineer, Forcepoint, **Garrett McNamara,** Principal Cyber Engineer, Forcepoint

APRIL 9 - SUNDAY

08:30 to 05:00	WS1	**CSX Cybersecurity Fundamentals (Day 2)** **Mike O. Villegas,** K3DES LLC
	WS2	**Web Application Security for Dummies (Hands on Workshop Day 2)** **Lee Neely,** Senior Cyber Analyst, Lawrence Livermore Laboratory, **Chelle Clements**, Senior Cyber Analyst, Lawrence Livermore Laboratory, **Jim McMurry,** CEO, Milton Security
	WS3	**Malware Analysis for Non-Programmers (Hands on workshop - Day 2)** **Peter Morin,** Principal Cyber Engineer, Forcepoint, **Garrett McNamara,** Principal Cyber Engineer, Forcepoint
	WS4	**Conquering the Risk Universe** **Shawna Flanders,** Director of Instructional Technology and Innovation, MIS Training Institute

Main Conference

APRIL 10 - MONDAY

	Accelerating Your Fundamentals	Cybersecurity Nexus	Security Emerging Issues, Tools & Techniques	IT Audit and GRC	Women In Techology
07:00 To 08:00	REGISTRATION and BREAKFAST BREAK sponsored by Ernst & Young, LLP				
08:00 To 10:00	**Opening Remarks: Debbie Lew**, Conference Chair ● **Keynote Speaker: The Game is Changing and How do We?, James Rinaldi** (CIO, NASA JPL) ● **Keynote Panel: "Women in Technology: Facing Today's Challenges While Building Tomorrow's Workforce"** Moderator: **Theresa Grafenstine**, Inspector General, U.S. House of Representative & Vice Chair, ISACA International Panelist: **Andrea Hoy,** CEO, A. Hoy and Associates and President of Information Systems Security Association (ISSA), **Gina Osborn**, Assistant Special Agent in Charge of the Cyber and Computer Forensics Programs, FBI, **Jeanne Holm**, Deputy CIO, Assistant General Manager, and Senior Technology Advisor, City of L.A., **Jessica Bair,** Senior Manager, Advanced Threat Solutions, CISCO				
	NETWORKING BREAK sponsored by TBD				
10:30 To 11:45	C1 **Risk Assessment Fundamentals** **Shawna Flanders,** MIS Training Institute	S1 **Introduction to Malware Analysis for Non-Programmers** **Peter Morin & Garrett McNamara,** Forcepoint	T1 **Toxic Access: What is it? Do you have it? Can you fix it?** **David Hawkins,** Centrify	G1 **DevOps: Driving Business Transformation; Where does GRC fit?** **Robert Stroud,** Forrester	W1 **Story Telling: Effective Communication** **Kimo Kippen,** Hilton Worldwide
	LUNCH NETWORKING BREAK sponsored by TBD CISO Luncheon sponsored by TBD (by invitation only)				
01:00 To 02:15	C2 **IT Audit Fundamentals Workshop – Part 1** **Jonathan Shelton,** Deloitte, LLP & **Frank Mariduena,** SCE	S2 **Board Concerns about Cyber and Technology Risks** **Rob Clyde,** ISACA	T2 **High Tech Cyber Crime Case Studies** **Donn Hoffman,** High Technology Crime Division & **Benyomin Forer,** Los Angeles County District Attorney's Office	G2 **Cloud Security — An IT Risk, Privacy & Compliance Program for SaaS** **Michael Sherwood,** City of Las Vegas, **Billy Spears,** Hyundai Capital America & **Thomas Phelps IV,** Laserfiche, **David Chen,** Director of IT & Security, Laserfiche	W2 **Soft Skills for Assurance Professionals** **Shawna Flanders** MIS Training Institute

Conference Schedule

	Accelerating Your Fundamentals	Cybersecurity Nexus	Security Emerging Issues, Tools & Techniques	IT Audit and GRC	Women In Techology
	NETWORKING BREAK sponsored by TBD				
02:45 To 03:45	C2 **Continued**	S3 **Cyber in Action: Technology Enablers IoT and Cloud** **Glenn Aga & Vinay Garg,** Deloitte	T3 **Securing a Cloud Generation by Protecting Information Everywhere** **Jerry Fraizer,** Symantec	G3 **A Call to Arms: Audit's Role in the (Ongoing?) Cyber War** **Theresa Grafenstine,** US House of Representative	W3 **WIT Panel: The Path to Leadership** **Cheryl Santor,** Retired, **Andrea Hoy,** ISSA, & **Janice Pearson,** Warner Brothers
	SESSION CHANGE				
04:00 To 05:00	C2 **Continued**	S4 **The Power of Trust: How Application Control Stops Ransomware and Malware** **Steven Shanklin,** White Cloud Security, Inc.	T4 **NIST SP 800-171 and CUI** **Mike Villegas,** K3DES LLC & **Chris Buthe,** California ManufacturingTechnology Consulting (CMTC)	G4 **Amazon Web Services: Auditing the next frontier in cloud computing** **Erin Relford, Devon Bleak,** 21st Century Fox	W4 **Personal Branding** **Kimo Kippen,** Hilton Worldwide
05:00 To 06:30	Opening Conference/Women in Technology Networking Reception Sponsored by TBD				
	APRIL 11- TUESDAY				
07:00	BREAKFAST BREAK sponsored by TBD				
08:30 To 09:45	**General Session** **The State of Cybersecurity** **Jessica Blair,** Senior Manager, Advanced Threat Solutions, CISCO				
	NETWORKING BREAK sponsored by TBD - EXHIBITION FAIR				
10:15 To 11:30	C2 **IT Audit Fundamentals Workshop– Part 2** **Dotun Olagundoye & David Phung,** PwC	S5 **Files and Emails - Avoiding the Next Wave of Breach Targets** **Jackie Brinkerhoff,** SailPoint Technologies	T5 **Safely Embracing the Cloud** **Rob Clyde,** ISACA & **Robert Stroud,** Forrester	G5 **Enhance IT Risk & Auditing through Maturity Models** **Rob Johnson,** Bank of America	W5 **Executive Presence** **Kristina Ridaoui,** City National Bank
	LUNCH NETWORKING BREAK sponsored by TBD - EXHIBITION FAIR				
01:00 To 03:45	**IT Audit Directors Forum** - by Invitation Only Moderated by **Marios Damianides,** Ernst & Young, LLP & **& Terry Grafenstine,** Inspector General				
01:00 To 02:15	C2 **Continued**	S6 **Using Incident Response Tactics to Enhance Enterprise Breach Awareness** **Joshua Theimer & Hao Wang,** Ernst & Young, LLP	T6 **The Coming Storm - The Internet of Things (IoT)** **Johnny Munger,** TCW Group	G6 **Re-engineering your GRC Program with COBIT5** **Shawna Flanders,** MIS Training Institute	W6 **Leadership – Building Collaborative Relationships to Drive Results** **Helen Norris,** Chapman University
	SESSION CHANGE				

Conference Schedule

	Accelerating Your Fundamentals	Cybersecurity Nexus	Security Emerging Issues, Tools & Techniques	IT Audit and GRC	Women In Techology
02:30 To 03:30	C2 **Continued**	S7 **Cybersecurity in a Trump Era** **Kapil Raina,** HyTrust	T7 **Protecting Controlled Unclassified Information (CUI) are you ready?** **Dennis Sheppard,** HRL Laboratories LLC	G7 **Data Governance and Privacy - What's The Connection** **Eric Read,** Honda	W7 **So, You're Interested in A Career in Cybersecurity** **Patricia Benoit & Piunik Adamian,** SCE
	NETWORKING BREAK sponsored by TBD - EXHIBITION FAIR				
04:00 To 05:00	C3 **Make Your Audit Analytics Output Usable and Beautiful** **John Lee,** SCE	S8 **Improving Cybersecurity Decision Making** **Mikhael Felker,** Farmers Insurance	T8 **Cloud Control Frameworks: Why do I care and which one should I use?** **Robert Stroud,** Forrester	G8 **SOC Overview, Changes, Benefits, and Preparation** **Louis Van Der Westhuizen,** BDO USA LLP	W8 **Inspiring Young Talent for Cyber Careers** **Lee Ann Kline,** STEM Advantage
	APRIL 12 - WEDNESDAY				
	BREAKFAST BREAK sponsored by TBD				
08:30 To 09:30	C4 **Security Governance in a Fast Paced World** **Cheryl Santor,** Retired-Metro Water District of So. CA & **David Alexander,** LADWP	S9 **3rd Party Vendor Cybersecurity Risk Assessments** **Patricia Benoit,** SCE & **Abi Medupin,** Southern California Edison	T9 **Data Security in a Multi-Cloud World: A Multi-Dimensional Challenge** **Ashwin Krishnan,** HyTrust	G9 **Cognitive Technology to Transform the Audit** **John Lee,** KPMG	W9 **"I don't know how you do it." The Myth of Having it All** **Kim Lamoureux,** RiSK Opportunities
	SESSION CHANGE				
09:45 To 10:45	C5 **Controls Testing and Monitoring** **Tibyasa Matovu,** PwC	S10 **Modern Day Cyber Threats? From ICS to IoT** **Peter Morin,** Forcepoint	T10 **An inside Out Approach to Security** **Robert Slocum,** Forcepoint	G10 **Governing without clear standards: Lessons learned from the trenches** **Ron Raether,** Troutman Sanders	W10 **Mentoring the Next Generation: Finding and Developing the "Hidden Figures"** **Cora Carmody,** Jacobs Engineering & **Nanxi Liu,** Enplug
	NETWORKING BREAK Sponsored by TBD				
11:15 To 12:15	C6 **Leveraging Data Analytics for Cybersecurity Audits** **Michael Kano,** Focal Point	S11 **Focusing Your Cybersecurity Program: A Risk Based Approach** **Scott Takaoka,** VerSprite	T11 **Out-Ninja, the Ninjas - How to Audit Cyber Effectively** **Lou Rabon,** Cyber Defense Group	G11 **Assurance with the NIST Cybersecurity Framework** **Nelson Gibbs,** East West Bank	W11 **Recruiting Women for IT** **Anna Carlin,** Fullerton College & **Dan Manson,** Cal Poly Pomona
	SESSION CHANGE				
12:30 To 01:30	C7	S12 **Taking AIM at Cyber Risk: A holistic approach aligned to business strategy** **Orus Dearman,** Grant Thornton LLP	T12 **Filling Security Gaps for Online and Mobile Applications** **Brian Deitch,** F5	G12 **People Make the Best Exploits – For Security and Compliance Risks** **Jennifer Cheng,** Proofpoint	W12

WS1

CSX Cybersecurity Fundamentals

Facilitator: Mike O. Villegas, Vice President, K3DES LLC

Introducing the Cybersecurity Fundamentals (CSX) workshop (Two-Day Course); Why become a cybersecurity professional? The protection of information is a critical function for all enterprises. Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies (IT). The CSX Fundamentals workshop is designed for this purpose, as well as to provide insight into the importance of cybersecurity, and the integral role of cybersecurity professionals. This workshop will also prepare learners for the CSX Fundamentals Exam.

Find more information about this certificate here:
www.isaca.org/cyber/Pages/Cybersecurity-Fundamentals-Certificate.aspx

Learning Objectives:
The Cybersecurity Fundamentals Certificate exam tests for foundational knowledge in cybersecurity accross five key areas:

- Cybersecurity concepts
- Cybersecurity architenture principles
- Cybersecurity of networks, systems, applications and data
- Incident responses
- The security implications of the adoption of the emerging technologies

WS2

Web Application Security for Dummies

Facilitator: Lee Neely, Senior Cyber Analyst, Lawrence Livermore Laboratory
Chelle Clements, Senior Cyber Analyst, Lawrence Livermore Laboratory
Jim McMurry, CEO, Milton Security

Web application security is in the forefront of the cybersecurity battleground. Business is conducted online worldwide. Web applications are the gateways to corporate information and assets that need protection. The web application layer is the hardest to secure because applications are often built from reused components that might not be designed with the appropriate level of security, or which may introduce vulnerabilities when used in combination. In this hands on class you will learn how to assess web applications and services using open source tools to discover vulnerable areas as well as how adversaries use this information to access and compromise systems. The skills acquired over the course of the workshop will be used to conduct a "capture the flag" exercise to reinforce the information learned. LAPTOP REQUIRED.

Learning Objectives:
- Understand How Web Applications Can Be Vulnerable
- Overview and definitions; What exploits to detect; application vulnerabilities; common code mistakes; Importance of taking advantage of vulnerabilities
- Understand Web Application Testing Framework

- Introduction to Web Testing Framework tools and overview of Samurai WTF
- Techniques for access and assessing web applications
- What is Fuzzing and how to use; How to map websites and the purpose; Man in the Middle use to inspect and change traffic
- Application vulnerabilities used to change behavior of web applications
- Cross Site Scripting (XSS), remote and local file inclusion to affect behavior; SQL Injection used to manipulate web apps
- Hands-on Lab: Map websites, learn structures, possible weaknesses - manually and with tools; Divulge credentials using fuzzing and password entry pages; Manipulate traffic using man in the middle attack; database coding weaknesses used to access applications to get to backend systems; Capture the Flag excercise to discover embedded flags within web applications.

WS3

Malware Analysis for Non-Programmers

Facilitator: Peter Morin, Principal Cyber Engineer, Forcepoint
Garrett McNamara, Principal Cyber Engineer, Forcepoint

With the consistent increase in the use of malware as an attack vector, having the ability to analyze worms, bots and trojans have become a necessity for organizations. Using in-the-wild samples, this hands-on lab will allow attendees to gain an understanding of the concepts and techniques necessary to analyze the malware they come across in their organizations. This session is ideal for information security professionals, auditors, and IT systems administrators that do not have a background in programming. This session is meant to teach students how malware works, how to identify it and how to understand the risk to their environment.

Topics include:

- What is malware? Review of various types.
- How criminals, nation states and hacktivists are using malware
- Review of basic Windows internals and the effects of malware on the operating system
- Static vs. dynamic malware analysis
- Understanding malware obfuscation (i.e. packing)
- Understanding malware behavior - how to detect and monitor
- Performing behavioral analysis of malware
- Understanding basic code analysis techniques
- Using sandboxing technology to analyze malware (i.e. Cuckoo)
- Analyzing malicious Microsoft Office (Word, Excel, PowerPoint) documents and malicious Adobe PDF documents
- Physical memory capture and analysis using Volatility
- Setting up a malware analysis lab - Tools and tricks
- Using tools to analyze malware such as OllyDBG, OllyDump, Process Monitor, Wireshark, RegShot, RedLine, REMNUX, etc.

Pre-Conference Workshops

WS4

Conquering the Risk Universe

Facilitator: Shawna Flanders, Director of Instructional Technology and Innovation, MIS Training Institute

This tailored and highly interactive course is designed to give attendees an overview of the Risk IT Framework and the basics of risk management along with pitfalls and opportunity generation.

At the end of the program the attendee should have a general understanding of key risk management concepts and how to facilitate a scenario based risk assessment and conquer the risk universe.

Topics include:

- Overview of IT Risk Management
- Risk Management / GRC Tools
- Collaboration techniques between IT and Enterprise Risk Management
- How to build an annual risk assessment program
- Why framework and standard adoption are important
- Risk identification and evaluation techniques
- Risk response techniques
- Risk monitoring techniques
- Risk Register, Risk Universe and Risk Profile

Track #1

Accelerating Your Fundamentals

Designed for the operational/financial auditor or anyone new to the information technology auditing, security and governance who want to learn the fundamentals to enable or change a new career or refresh knowledge.This track provides the participants with the concepts, methodologies and techniques to help improve upon their knowledge, expertise and skills. Selected session proposals will provide participants with value–added tools such as audit programs, checklists, white papers and other reference material.

Track #2

Cybersecurity Nexus

In this track, cutting-edge IT and cybersecurity issues will be discussed along with recommendations and solutions. Topics include issues and risks related to social media, mobile technology risks (BYOD) IAM, cybersecurity governance, cloud computing strategies, threats to privacy as well as internal controls and Sessions are designed to include the latest cybersecurity topics to enhance the skills of audit, cybersecurity, and IT professionals.

Track #3

Security Emerging Issues, Tools & Techniques

Through demonstration and discussions of real world issues and applications of solutions, this track will help assurance, security and risk professionals understand emerging security risks to the business and operational environments, as well as relevant security techniques and tools. Sessions include topics that will enable participants to take away security ideas and techniques that will enhance their professional development and work.

Track #4

IT Audit and GRC

This track explores the concepts and terminology of emerging issues related to IT governance, frameworks and risk management. Included in this track is the ISACA research and tools designed and developed to aid the IT professional in recognizing today's emerging issues and mitigating impact on the enterprise. Sessions also include governance topics that supports the enterprise's IT ability to sustain and extend the organization's strategies and objectives.

Track #5

Women In Techology

Learn, get inspired and network from women leaders in technology. This track is open for all as we discuss about techniques and methods to be a successful leader. Hear from our women technology leaders on emerging issues. Additional topics included enhancing executive presence, techniques to develop and build personal branding, and establishing trust in the ever challenging environment. Men are welcome to attend.

Accelerating Your Fundamentals

C1 Risk Assessment Fundamentals

Speaker **Shawna Flanders**
Director of Instructional Technology and Innovation, MIS Training Institute

Risk Management is the primary process organizations can use to determine their current capability to identify, manage and respond to risk and a properly conducted risk assessment gives organizations the best depiction of their ability to maintain the confidentiality, integrity and availability of their information assets.

In this session, we will explore several of the more common risk assessment/analysis requirements for meeting both regulatory and industry requirements.

After completing this session, participant will be able to:

- Understand key components of the Risk Management Strategy
- Discuss the Risk Identification Process
- Examine Risk Assessment (including Maturity and Third Party Assessments)
- Explore Risk Response Process and Treatment Options
- Describe Good Practices in Risk Monitoring and Reporting

C2 IT Audit Fundamentals Workshop

Speakers (Part 1)

Frank Mariduena
IT Governance Manager, SCE

Jonathan Shelton
Manager, Deloitte

Speakers (Part 2)

Dotun Olagundoye
Manager, Risk Assurance, PwC

David Phung
Manager, Risk Assurance, PwC

In this two part workshop, participants will learn about IT auditor roles and relationships as well as the overall IT audit process from initial risk assessments through the development and use of control frameworks. This class is targeted toward IT auditors who are new to the profession, financial auditors learning IT audit, integrated auditors or IT personnel who are transitioning into greater involvement in IT audit. We will discuss the methodologies and frameworks that support IT audit such as COBIT® 5, general computing controls, application level controls, and how the Sarbanes-Oxley Act of 2002 affects the IT auditing profession. Participants will have the opportunity to apply acquired knowledge by the end of the workshop.

After completing this session, the participants will be able to:

- Understand the principles and practices of IT auditing,
- Understand the standards, guidance and procedures that ISACA recommends
- Understand IT auditors role, the audit process and drivers, regulatory requirements (e.g., SOX, PCI, privacy), and the role of frameworks/methodologies (e.g., COBIT® 5/ITIL/ISO17799)
- Understand IT risk assessment, developing the IA plan and conducting the audit
- Understand strategy & planning, business continuity, relationships with outsourced providers
- Understand applying COBIT® 5 in audits
- Understand information security,
- Understand computer operations and change management (e.g., SDLC, change control)
- Understand application controls and the IT auditor's role in business process audits.

C3 Make Your Audit Analytics Output Usable and Beautiful

Speaker **John Lee**
Senior Analyst/Data Scientist, Southern California Edison

While the best audit analytics can work wonders, they can't speak for themselves in boardrooms. And audit/assurance/compliance professionals too often fall short in articulating what they've done. That's hardly surprising; companies hiring for technical roles rightly prioritize technical expertise over presentation skills. But mind the gap, or face the consequences. Even the best audit analytics results could be ignored by management and the Board if they don't convey clearly and convincingly the insights on risks, exposures and impacts to the well-being of the enterprise.

We're all human after all, and appearances matter. That's why a beautiful interface will get you a longer look than a detailed narrative with an uneven personality. That's also why the elegant, intuitive usability of products like the iPhone or the Nest thermostat is making its way into the enterprise. Audit analytics should be consumable, and best-in-class organizations now include designers on their core analytics teams. Management and the Board will respond better to interfaces that make key findings clear and that draw users in.

In this session, we will demonstrate examples of dashboards developed using Tableau that present data analytics results in an intuitive, succinct and beautify way.

After completing this session, the participants will be able to:

- Learn the principles of presenting audit analytics results in an intuitive, beautiful fashion
- Avoid the common pitfalls in presenting audit analytics results on a dashboard
- Be exposed to the state-of-the-art data visualization techniques

C4 Security Governance in a Fast Paced World

Speakers **Cheryl Santor**
Information Security Specialist, Retired

David Alexander
Information Security Specialist, Director of Information Security,
Los Angeles Department of Water & Power

We work in fast paced environments where Governance is overlooked in setting up the next application or systems. Management wants to provided a solution at a pace where governance is not addressed and is an after thought. Can you go back and provide Governance once a system or application is in place? Examples of how this can be done. In an ideal world everything would be in place prior to rollout of an application or system, but we know that the wheels in motion behind governance are not always ready when the deadline is facing the corporation, how to provide a governance model even with challenges.

After completing this session, the participant will be able to:

- Understand how to keep some level of Governance around applications, systems and procedures in a fast paced environment.
- Understand what to do if a framework is not in place to comply with a Governance model?
- Understand how to promote a Governance environment in your workflows.
- Identify what risks do you encounter without a Governance model of some type in your organization?
- Understand what can you do as a single person to speak up and convince management Governance is necessary.

C5 Controls Testing and Monitoring

Speaker **Tibyasa Matovu**
Director, Risk Assurance, PwC

Controls Testing and Monitoring helps in establishing, monitoring and testing controls across the organization. Learn how to design and implement continuous monitoring and testing programs that enabling organizations to have oversight of critical regulatory compliance programs. You will explore how to leverage analytics for testing, how to design testing scripts, and use delivery centers to test controls across the 1st, 2nd and 3rd Lines of Defense.

After completing this session, the participants will be able to:

- Understand how to design and implement continuous monitoring and testing
- Leverage continuous monitoring and testing for oversight of critical regulatory compliance programs
- Leverage analytics for testing
- Design testing scripts
- Use delivery centers to test controls across the first, second and third lines of Defense

C6 Leveraging Data Analytics for Cybersecurity Audits

Speaker **Michael Kano**
Senior Manager Data Analytics, Focal Point

Not a month goes by without large organizations notifying the public that they have been the victims of cyberattacks. Hackers, while often motivated by the challenge of penetrating a well-known network, are also capturing account information that can include PII. This data is often traded and can end up in the hands of individuals and organizations far removed from the original attacker.

After completing this session, the participants will be able to:

- Understand the nature of cybersecurity risks and their costs
- Be aware of the types of tests that can be run using desktop data analytics tools such as ACL, IDEA, Arbutus, and Alteryx
- Learn how other audit organizations are addressing cybersecurity risks.ary.

S1 Introduction to Malware Analysis for Non-Programmers

Speakers

Peter Morin
Principal Cyber Engineer, Forcepoint

Garrett McNamara
Principal Cyber Engineer, Forcepoint

With the consistent increase in the use of malware as an attack vector, having the ability to analyze worms, bots and trojans have become a necessity for organizations. Using in-the-wild examples, this presentation will allow attendees to gain an understanding of the concepts and techniques necessary to analyze the malware they come across in their organizations.

Topics include:

- What is malware? Review of various types.
- How criminals, nation states and hacktivists are using malware
- Static vs. dynamic malware analysis
- Understanding malware behavior - how to detect and monitor
- Understanding code analysis techniques
- Setting up a malware analysis lab - Tools and tricks
- Using tools to analyze malware such as OllyDBG, OllyDump, Process Monitor, Wireshark, RegShot, Volatility, etc.

S2 Board Concerns about Cyber and Technology Risks

Speaker

Rob Clyde
International Vice President and Board Director, ISACA

The C-suite and boards of directors are increasingly concerned about cyber attacks and riks. In addition, they are anxious to understand the business impact and ensure appropriate risk management relative to new technologies. This session will explore new technologies include the Internet of Things, artificial intelligence and machine learning, augmented reality and virtual reality, cloud, and Big Data. In addition, cyber attacks continue to escalate with data breaches and RansomWare attacks being discussed at the board level. This session will explore likely questions your board will ask you and discuss how board might address and deal with these issues.

After completing this session, the participant will be able to:

- Better understand business impact of new technologies and cyber risks
- Understand board perspective relative to cyber and new technologies
- Be prepared for likely questions the board will ask
- Better articulate risks and options to the board of directors and C-suite

S3 Cyber in Action: Technology Enablers IoT and Cloud

Speakers

Glen Aga
Managing Director, Cyber Risk, Deloitte

Vinay Garg
Senior Manager, Cyber Risk, Deloitte

The Internet of Things (IoT) and shift to the cloud offers new ways for businesses to create value, however the constant connectivity and data sharing also creates new opportunities for information to be compromised. Explore some of the more notable developments in the battle to combat cyber risks. Join Cyber Risk consultants from Deloitte to discuss cyber risks and mitigations for two trending technology enablers: Cloud and IoT. Glenn Aga and Vinay Garg will present general concepts relating to how to adapt your cyber security approach to incorporate these two trending technology enablers we see moving in the marketplace.

S4 The Power of Trust: How Application Control Stops Ransomware and Malware

Speaker

Steven Shanklin
CEO & Founder, White Cloud Security, Inc.

Homeland Security's US-CERT recommends "App Control as the #1 Malware Mitigation Strategy. What is this technology, and how does it block what Antivirus can't?

Hackers are winning the cyberwar and the global impact of malware has exceeded $3 Trillion and is now more profitable than the global drug trade in marijuana, cocaine and heroin combined. The cost of Ransomware in Q1 2016 was $209 Million. Almost a 3,500% increase from 2015. Application Control is the number one type of breach prevention solution recommended by Dept. of Homeland Security's US-CERT, Australia's ASD, Canada, AIG, SANS, ISA, and NACD. It's the only effective solution to the rapidly expanding array of today's ransomware and malware threats.

After completing this session, the participant will be able to:

- Understand what Ransomware and Malware are and what hackers hope to accomplish by using them against businesses and government organizations.
- Understand why Ransomware and Malware can't be completely stopped by traditional antivirus, sandboxing, heuristic learning, machine learning, behavior analysis, big data and other next generation antivirus technologies.
- Understand the Application Control technology paradigm shift and how it works to prevent malware from running and why it a 100% effective solution that other antivirus technologies can't match.
- Understand why Application Control hasn't been widely adopted and what have been its barriers to deployment and management.

S5 Files and Emails - Avoiding the Next Wave of Breach Targets

Speaker **Jackie Brinkerhoff**
Director, Market and Product Strategy, SailPoint Technologies

2016 was hammered with security breaches like never before farther-reaching, more voracious and aimed at new targets: emails, files and other types of unstructured data. Unstructured data is information that resides outside of a typical database, such as documents, spreadsheets and even internal portals. Unstructured data is incredibly challenging to manage because it can be easily saved in multiple places (inside and outside the corporate walls) and shared via email.

It's widely accepted that about 80% of an organization's data is unstructured which presents a huge challenge for companies like yours. Attend this session to learn why unstructured data is so difficult to protect, why it should be a top priority in your identity governance program, and how SailPoint can help mitigate unstructured data risks in less than one month.

After completing this session, the participants will be able to:

- Understand how to identify sensitive unstructured data within your organization
- Learn how to avoid the typical pitfalls associated with securing access to data
- Discover how to address critical compliance requirements centered around data access
- Realize how cloud migration strategies (e.g. Office365, SharePoint, Box, etc) are impacted by unstructured data.
- Identify ways to easily engage and empower business data owners in your data access governance program while alleviating IT burden.

S6 Using Incident Response Tactics to Enhance Enterprise Breach Awareness

Speakers **Joshua Theimer**
Senior Manager, Ernst & Young

Hao Wang
Manager, Ernst & Young

Publicly disclosed breaches reveal an unnerving pattern: companies are reactive, waiting for security alerts to trigger response. Even when alerts ever do sound, a surprising number lack the fundamentals needed to build and develop a comprehensive understanding of the incident. We will demystify the process and give you the background needed to tackle this head on.

After completing this session, the participant will be able to:

- Identify indicators of real world tactics used by attackers on internal networks
- Use artifacts to enhance current enterprise monitoring capabilities typically neglected by traditional security tools
- Understand how to quickly determine the extent of a compromise

S7 Cybersecurity in a Trump Era

Speaker **Kapil Raina**
Vice President, Product Marketing, HyTrust, Inc.

With a new U.S. President taking office -- a new cybersecurity era will also dominate the corporate and political landscape. CIO, CISOS, and Auditors all still need to be ready to respond to security threats and changing regulatory landscape quickly. This session will help audiences identify this potential changes and provides best practices to deal with them.

How will cybersecurity standards and responses change in a Trump administration?

After completing this session, the participant will be able to:

- Understand what are some expected outcomes: technology (especially encryption), policy (cyber offensive, legal), infra structure (changes for providers and large enterprises)
- Understand how to position to deal with the outcomes including best practices that will allow for an uncertain future

S8 Improving Cybersecurity Decision Making

Speaker **Mikhael Felker**
Director, Information Security Risk Management, Farmers Insurance

Information Security, Risk and Audit leaders require excellent decision-making skills. There is a continuous stream of new threats, new vulnerabilities, and new technologies that require our attention.

However as professionals in this field there are a number of cognitive biases that impair our judgment in making decisions. Examples of this include confirmation bias, availability bias, recency bias, loss aversion and many others. In this talk we will dive into how these biases are impacting security programs and investments, and what we can do to improve our decision-making for better outcomes.

After completing this session, the participant will be able to:

- Understand what common cognitive biases are
- Understand how biases affect our decision-making and outcomes
- Understand what can be done to reduce bias and improve decisions

S9 3rd Party Vendor Cybersecurity Risk Assessments

Speakers

Patricia Benoit
Senior Manager, Cybersecurity Compliance, SCE

Abi Medupin
Senior IT Specialist Cybersecurity and IT Compliance, Southern California Edison

As business organizations increase the use of outside vendors for IT services, it is important that cybersecurity risk be considered prior to purchasing solutions. However, the business may be more focused on speed of delivery than managing risk. Cybersecurity functions are building risk awareness, and are also learning that risk is best balanced with business need. In an effort to strike this balance, organizations are looking at risk-based models that allow cybersecurity risk assessments to be tailored. Early screening of cybersecurity risk to sensitive data and systems maximizes business and IT resources by focusing on the highest risk areas, at the right point in time. This approach allows the business and IT to partner to provide solutions through-out the procurement lifecycle, while ensuring that funding is applied to solve priority business problems.

After completing this session, participants will be able to:

- Understand how a risk-based approach is able to effectively screen sensitive data and technology architecture risk
- Apply resources to the highest risk areas throughout the procurement lifecycle

S10 Modern Day Cyber Threats? From ICS to IoT

Speaker

Peter Morin
Principal Cyber Engineer, Forcepoint

This presentation will discuss the modern cybersecurity threats that plague our population today and that would have the most direct impact on our lives. Almost everything we do today uses technology in some way and most if not all are interconnected or will be in the near future. Technology such as IoT allows us maintain our well-being such as tracking our fitness goals or monitoring our insulin. We are making our cities smarter by implementing traffic congestion systems and better mass transit management and ensuring the availability of metered electricity and clean water through industrial control systems (ICS). However, this all comes at a cost. Just as this technology has become a necessity in our lives, it has also become a prime target for cyber-attack.

After completing this session, participants will be able to:

- Understand the security of IoT and some well-known examples of cyber risk (i.e. baby monitors, insulin pumps, home appliances, automobiles, etc.)
- Understand the security of ICS including the risks related to power generation, water management and the smart city movement
- Gain exposure to the methods that security professionals, auditors, etc. can use to assess these various technologies to better understand the risks associated with their use

S11 Focusing Your Cybersecurity Program: A Risk Based Approach

Speaker **Scott Takaoka**
Vice President, Business Development, VerSprite

Cyber attacks are coming from all directions. Phishing, web app attacks, IoT, social engineering ploys, and the list goes on. Logical and physical domains are in play, and yet your budget and headcount are limited. Where do you focus? Are âbest practices truly best for you?

Come to this session where you will learn about a new risk management concept The Organizational Threat Model. Organizational Threat Modeling is a technique that aligns your organizational threats, distills them into attacks then analyzes your security controls and the operational damage that an incident can cause. By taking an offensive and defensive perspective, you can more accurately evaluate the effectiveness of all of the aspects of your security program, and prioritize initiatives based on business impact and likelihood.

After completing this session, the participants will be able:

- Learn about an operational risk based approach to evaluate security program effectiveness
- Gain exposure to a methodology that will help identify the top threats to your organization and understand the effectiveness of your controls
- Understand a way to provide contextual based analysis to your risk management program in addition to framework based approaches
- Learn how a modeling approach can help tailor threat intelligence, penetration testing, and incident response programs based on threats

S11 Taking AIM at Cyber Risk: A holistic approach aligned to business strategy

Speaker **Orus Dearman**
Managing Director, Risk Advisory Services, Grant Thornton LLP

Most organizations take the wrong approach to cyber risk.
The digitization of currencies, transactions, relationships, experiences and assets has transformed entire industries.
But with digital innovation comes new risk, and cyber risk management should be properly implemented in an integrated risk management and risk governance program.

A holistic approach is best organized by means of a framework that helps management identify roles, responsibilities, relationships and other relevant factors. It enables management to:

- Place cyber risks in a strategic context
- Link cyber risks to growth and performance
- Rationalize practices and spend.
- Make better business decisions

After completing this session, the participants will be able to;

- Learn leading practices for looking at cyber risk in strategic business context
- Learn how to action for results.

Security Emerging Issues, Tools & Techniques

T1 Toxic Access: What is it? Do you have it? Can you fix it?

Speaker **David Hawkins**
Senior Systems Engineer, Centrify

This session is a discussion on the concepts of toxic access, with some practical real world advice you can apply to your people training, process management, and technical automation. This is a non-product focused topic, but examples may be used from the Centrify product as an illustration of one way to actually accomplish this goal in a real solution.

After completing this session, the participants will be able:

- Understand the concepts behind Toxic Access
- Learn a few simple steps to identify toxic access in existing user accounts and groups
- How Auditors test for Toxic Access
- Some suggested steps to remedy toxic access
- See a live solution that can control toxic access conditions
- Understand how this kind of access management ties back to industry knowledge and best practices specifically outlined in the ISC2 Body of Knowledge

T2 High Tech Cyber Crime Case Studies

Speakers **Benyomin Forer**
Deputy District Attorney, High Technology Crime Division,
Los Angeles County District Attorney's Office

Donn Hoffman
Deputy District Attorney, High Technology Crime Division,
Los Angeles County District Attorney's Office

Prosecutors from the Los Angeles County DA's office High Technology Crime Division will discuss the role of law enforcement in incident response and data breach situations. They will demonstrate emerging issues pertaining to technological crimes as well as bring awareness to the community on potential cyber threats.

After completing this session, participants will be able to:

- Understand emerging issues pertaining to technological crimes
- Gain awareness as part of the community on potential cyber threats
- Know when and how to report an incident to law enforcement
- Learn about recent cybercrime cases prosecuted in Los Angeles.

T3 Securing a Cloud Generation by Protecting Information Everywhere

Speaker **Jerry Fraizer**
Senior Sales Engineer, Symantec

As the information age continues to explode at an exponential rate more organizations are moving their digital assets to the cloud. The benefits of moving to the cloud go well beyond cost savings and scalability. The cloud also enables today's mobile and flexible workforce new ways to collaborate and be more productive that weren't possible with the constraints of traditional technology infrastructure. Security has long been thought to be the weakest link or Achilles heal for organizations that are adopting a cloud strategy. This talk will cover new approaches that are being leveraged to protect information everywhere as organizations enter into the cloud generation.

After completing this session, the participants will be able to:
- Better understand how multi vector threats are crafted
- Better understand the cloud kill chain
- Better understand their organizations use of cloud applications
- Identify risky behaviors associated with cloud application usage
- Identify was to better secure company and personal devices
- Better understand how to protect information everywhere it might be used

T4 NIST SP 800-171 and CUI

Speakers **Miguel (Mike) Villegas**
Vice President, K3DES LLC

Chris Buthe
Cybersecurity Specialist, California Manufacturing Technology Consulting (CMTC)

On November 4, 2010, the President signed Executive Order 13556, Controlled Unclassified Information(CUI) to standardize the way the executive branch handles unclassified information that requires protection and designated the National Archives and Records Administration (NARA) as the Executive Agent to implement that program. On September 14, 2016, NIST SP 800-171r1 (Controlled Unclassified Information in Nonfederal Information Systems and Organizations) was formally issued to provide guidance on CUI safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.

Non-Federal entities include a State, interstate, Indian tribal, or local government, as well as private organizations. Private organizations are government contractors, universities, service providers, and entities that store, process and transfer CUI.

Non-compliance by December 31, 2017 means government contractors will lose their contract. Experience has shown this order is not being taken seriously. This session will focus on the NIST SP 800-171 control families, requirements, and compliance dates.

After completing this session, the participant will understand:
- Controlled Unclassified Information
- What is a non-federal entity subject to NIST SP 800-171
- CUI classification required in FIPS 199
- The 14 control families in NIST SP 800-171
- he basic and derived requirements in the NIST SP 800-171
- Impact of non-compliance for non-federal entities

T5 Safely Embracing the Cloud

Speakers

Rob Clyde
Board Director, ISACA

Robert Stroud
Principal Analyst, Forrester Research

Where does the cloud meet security and compliance? Public cloud and SaaS providers have significant investments in human capital, resources, process and tooling to assure that their clients are secure and compliant in the cloud? In fact, often moving workloads to the cloud may improve an organizations' IT governance, compliance and security posture. For example, backup and disaster recovery may be simplified and the risk from Ransomware lessened. That said you cannot abdicate accountability and there is still work to be done. Where does the cloud vendor's responsibility stop and your enterprise's start? How can you address the likely security issues and risks a move to the cloud incurs

After completing this session, the participant will be able to:

- Explain the state and drivers of cloud adoption.
- Understand key considerations of moving to cloud.
- Explain why cloud may improve security and GRC.
- Understand 3rd party cloud provider risk.

T6 The Coming Storm - The Internet of Things (IoT)

Speaker

Johnny Munger
CISO, TCW Group

The Internet of Things (IoT) is still the early stages and has a lot of hype and is has gained the attraction of many researchers and that also includes hackers. Meanwhile, supplying privacy and security is an inseparable part of this technology. Without providing enough security, the promising benefits of this new and flourishing technology could be misused. In this session, I will first give a brief overview of IoT and then we will go through more details about the current challenges and provided some tools to help to provide security for finding and understanding IoT. Because IoT devices provides a platform for communication between objects and where objects can be organized and managed via the Internet this will become a fertile area for hackers.

After completing this session, the participant will be able to:

- Better understand how attacks on Internet of Things (IoT) devices will increase due to growth in the number of connected objects, poor security hygiene, and the value of data on IoT
- Leverage various tools and techniques to discover IoT devices
- Better understand how IoT could be used to attack or ride inside your employee’s access or your vendor's access into your company’s network

T7 Protecting Controlled Unclassified Information (CUI) are you ready?

Speaker **Dennis Sheppard**
Senior IT Porject Manager, HRL Laboratories LLC

With the December 31, 2017, compliance deadline for DFARS 252.204-7012 and the NIST 800-171 rapidly approaching is your organizations ready? For the smaller organization, implementation of NIST SP 800-171 can seem like an overwhelming challenge. In this session you will share in one small organizations journey to compliance.

After completing this session, the participants will be able to:

- Understand how to validate your controls, what customer are asking for.
- Lessons learned what you should be aware of and what you might avoid.
- Understand the impact on small and medium compaines

T8 Cloud Control Frameworks: Why do I care and which one should I use?

Speaker **Robert Stroud**
Principal Analyst, Forrester Research

The transition to cloud computing is underway and the velocity is increasing with cloud providers offering more compliance and security certifications every day. That said, the compliance delivered by the providers supplements, rather than replaces an effective, and often mandated, compliance requirements for your organization.

This session will discuss where the growth in cloud and will provide an overview of a number cloud control frameworks including:

- ISO 27017
- FedRAMP
- Cloud Security Alliance
- COBIT for Cloud Assessment

The session will provide you with a good baseline as you return to the office allowing you to accelerate your role in the cloud journey.

After completing this session the participant will be able to:

- Understand the velocity of the current transformation to the cloud, which industries and applications are transitioning
- Understand the basics of the most frequently used Cloud Control Frameworks and their differences
- Understand control boundaries between cloud providers and the organization
- Articulate the role value of automated controls in the delivery of business technology

T9 Data Security in a Multi-Cloud World: A Multi-Dimensional Challenge

Speaker **Ashwin Krishnan**
SVP, Product & Strategy, Hytrust

There is no question that a multi-cloud environment is fast becoming the dominant IT model of the future, and securing data in this new model has emerged as one of the top challenges for most organizations. If data security used to be a serious challenge when all your data was in one place, what does it now mean to have that data spread across multiple places; from private data centers to hosting partners, to a variety of cloud service providers. And to further complicate matters, your organization is probably required to comply with an ever-increasing set of industry and government mandated regulations across all these different cloud environments. We have fundamentally gone from a one-dimensional data security nightmare to a multi-dimensional data security nightmare!

Join this session and learn about how this new reality can impact your organization's data security posture, even with the right security technologies in place such as encryption and key management.

After completing this session, the participants will be able to:

- Understand that not all clouds are created equal
- Understand the obligation of the cloud provider and the enterprise and how this varies per cloud
- Understand that data encryption is only part of the solution
- Understand that in a hybrid world the types of encryption and key management solutions are vast and can be easily misunderstood if not evaluated carefully
- Ask the right questions of their provider when it comes to complete lifecycle management of keys and understand this can be done easily by themselves as well

T10 An inside Out Approach to Security

Speaker **Robert Slocum**
Forcepoint

The security industry has historically focused on point products to stop threats. Despite an industry wide spend of $86 billion dollars a year, data breaches have not stopped. In fact, the attacks have increased in both frequency and size. Perhaps the biggest problem is our reactive focus on the attack itself, instead of focusing on the data and the very users who access that data. In an inside out approach to security, we demonstrate how organizations can go beyond simply blocking a file from leaving through a channel, to gaining unrivaled visibility into users' actions and context around the user behavior. We will demonstrate how Behavioral and Security Analytics are helping mitigate risks while easing the burden on IT Security staffs by automatically identifying the users and data incidents that pose the greatest risk to organization.

After completing this session, the participants will be able to:

- Think differently about security. Instead of focusing on threats and technology, security professionals should start looking at the intersection of people and data
- Understand the different types of insider threats, whether they be malicious insiders, accidental users, or compromised systems
- Learn how behavior and security analytics are helping mitigate risks while easing the burdern on IT Security Staffs

Security Emerging Issues, Tools & Techniques

T11 Out-Ninja the Ninjas - How to Audit Cyber Effectively

Speaker **Lou Rabon**
CEO, Cyber Defense Group

Cybersecurity is a complex topic, and the landscape is constantly changing. Auditors are increasingly faced with the task of auditing organizations against a set of standards that might exceed their core competency. Cybersecurity is not black or white and audits need to be. In this course, you will l earn how to determine what the important areas are to concentrate on, using risk as a guide. You'll also learn how to deal with smokescreens and what to do when faced with technical items and evidence.

After completing this session, the participants will be able to:

- Overcome technical shortcomings to audit effectively
- Determine what evidence to look for and understand when it is invalid
- Understand what areas are important to focus on from a cybersecurity perspective

T12 Filling Security Gaps for Online and Mobile Applications

Speaker **Brian Deitch**
Security Enginer, F5

Learn about the two most common and dangerous forms of computer fraud: malware and phishing. You'll learn about how these forms of fraud are created and the danger they cause to organizations and their customers.

After completing this session, participants will be able to:

- Learn how F5 WebSafe helps organizations detect fraud
- Keep their own customers safe from malware and phishing attacks

G1 DevOps: Driving Business Transformation; Where does GRC fit?

Speaker **Robert Stroud**
Principal Analyst, Forrester

Technology is rapidly dismantling long-established business models and creating new ones in their place. Every business today is being driven to drive velocity and agility to compete and drive differentiation. Consumers, empowered by these rich application interactions, have never had more power or choice.

DevOps is a set of practices and cultural changes supported by the right tools that creates an automated software delivery pipeline, enabling organizations to win, serve, and retain these consumers. To differentiate your business from others, you must use these methods to build in quality and become more nimble.

This session will discuss what DevOps is and how it is transitioning organizations their business objectives and how Governance, Risk, Compliance and Security will fit into the new world where velocity and agility are driving execution.

After completing this session, the participants will be able to:
- Understand what DevOps its components
- Understand where DevOps is transforming my business
- Where GRC fits into the DevOps Pipeline
- How Continuous Deployment will change the manner we work

G2 Cloud Security - An IT Risk, Privacy & Compliance Program for SaaS

Speakers

Michael Sherwood
Director of Technology & Innovation, City of Las Vegas

Thomas Phelps IV
Vice President of Corporate Strategy & CIO, Laserfiche

Billy Spears
Chief Privacy Officer, Hyundai Capital America

David Chen
Director of IT & Security, Laserfiche

These days, cybersecurity dominates headlines and has become a topic of board room discussions. Yet, today's digital business demands that companies continue to invest in Cloud-based technologies to rapidly scale IT services. In this session, executives from the private and public sectors will share how they implemented IT risk, privacy and compliance programs in response to the shift to Cloud services, and what other organizations should consider to be compliant with the current regulatory landscape.

The session will include:
- City of Las Vegas' move to a "cloud first" strategy and the security implications of transitioning enterprise applications to the Cloud.

- Hyundai Capital America (HCA)’s implementation of a privacy program that addressed key privacy requirements— including the new EU-U.S. Privacy Shield data sharing framework and California’s new online reporting tool for violations of the California Online Privacy Protection Act (CalOPPA).
- Laserfiche’s introduction of Laserfiche Cloud, a SaaS-based enterprise content management solution, which created additional security requirements for its business.
- Lessons learned on how each company addressed significant IT risk, security and privacy requirements—and what you should be aware of for your company.

G3 A Call to Arms: Audit's Role in the (Ongoing?) Cyber War

Speaker

Theresa Grafenstine
Inspector General, US House of Representatives

Every day, we hear news reports of another organization being breached. We find ourselves asking, Who's Next? The stakes are too high for audit to wait until after a breach occurs to conduct a post-mortem of the attack. To provide value and to possibly protect our organizations from failure, audit needs to be proactive.

After completing this session, the participants will be able to:

- Understand classic breach tactics
- Describe what good security and controls look like
- Discuss how the US House of Representative Office of Inspector General has taken a proactive role in helping the House to address cyber threats.

G4 Amazon Web Services: Auditing the Next Frontier in Cloud Computing

Speakers

Erin Relford
IT Audit Manager, 21st Century Fox

Devon Bleak
Director, Cloud Engineering, 21st Century Fox

Has your IT department's adventure into Amazon Web Services felt like a Jump Program straight out of The Matrix? Is your company thinking of joining the millions already invested in AWS? If yes, then this course is designed for you. This Inception like discussion will delve into the parallels of Amazon Web Services' shared security model, the relationship between the business who dreams up the plan, IT who architects the infrastructure, and how AWS has turned traditional audit on its head.

This class is targeted toward IT auditors new to AWS and IT professionals interested in engaging governance at every layer of development and operations. We will discuss the responsibilities between customer and vendor, how to prevent becoming an AWS horror story, and how to approach auditing Amazon Web Services.

After completing this session, the participant will be able to:

- Understand your IT function's role in AWS security
- Apply audit principles to Identity and Access Management in AWS
- Evaluate security goups in AWS
- Assess VPC and use of other AWS services with a governance perspective

IT Audit, Governance, Risk and Compliance (GRC)

G5 Enhance IT Risk & Auditing through Maturity Models

Speaker **Rob Johnson**
Senior Vice President, Bank of America

Managing maturity provides a systematic planning and prioritization methodology for organizations to optimize and streamline its resources. Maturity models is an enabler to quality risk based approaches. Although many organizations state their approach is risk-driven, many lack a systematic maturity model approach to discuss the issues with regulators and auditors using a common language and frame of reference. This session coves foundational understanding of maturity models (including CMMI, ISO15504, FAIR, and others), synergies with COBIT 5, and real-life success stories. With ISACA's acquisition of CMMI® Institute, this session is timely to understanding major trends and emerging industry techniques to improve understanding of IT risk and better prepare for audits.

After completing this session, the participants will be able to:
- Learn how maturity models can be used to enhance understanding of IT risk
- Learn now maturity models can be used to understand control coverage
- Improve IT risk and audit planning with maturity model

G6 Re-engineering your GRC Program with COBIT5

Speaker **Shawna Flanders**
Director of Instructional Technology and Innovation, MIS Training Institute

This session is designed to give GRC professionals and auditors a roadmap for assessing their current GRC program and optimizing it using COBIT 5.

At the end of the course the attendees should have a better understanding of COBIT 5 and how to integrate it into your GRC program to reduce the impact to the business and IT resources within your enterprise.

After completing this session, the participants will be able to:
- Understand COBIT 5 principles, governance and management
- Understand COBIT 5 process reference model
- Understand COBIT Enablers
- Understand COBIT5 Implementation Life Cycle
- Leverage COBIT 5 to optimize their GRC Program

G7 Data Governance and Privacy - What's The Connection

Speaker **Eric Read**
Honda

Each year in the United States and around the world regulations are enhanced to further protect citizens and nations form those wanting to gain from others. This course will focus Data Governance and Data Privacy and what its designed to heighten an Auditor’s knowledge of Data Privacy and Data Governance using common business language. During the course, we will discuss some of the known vulnerabilities, threats and risks facing today's enterprise or agency and some of the more common controls used to safeguard data, despite its form.

By the end or our course attendees will gain a broad base understanding of data governance and data including incorporating Data Privacy and Data Governance components into every audit engagement.

After completing this session the participate should have a greater understanding regarding:
- Data Privacy Fundamental’s
- Understand data governance fundamental’s
- Understand basic control suite
- Be familiar with auditing privacy and data governance

G8 SOC Overview, Changes, Benefits, and Preparation

Speaker **Louis Van Der Westhuizen**
Director, Third Party Attestation, BDO USA LLP

As cloud computing service models gain widespread adoption among companies looking for cost-effective, efficient technology solutions, such companies are demanding high levels of assurance from these service providers about the integrity, accuracy, and reliability of the services being provided to them, especially when sensitive financial, private, and confidential data are involved. Such assurance is critical for risk management and mitigation at user entities - which retain responsibility for any outsourced services.

In highly regulated industries like financial services, third-party compliance isn’t a nice-to-have; it’s a must-have. The Consumer Financial Protection Bureau, the Office of the Comptroller of Currency (OCC), and other regulators have shared explicit examination guidance on third-party risk management. The OCC actually mandates that banks stipulate the types and frequency of audit reports in contracts with third parties. Similarly, in the healthcare industry, business associates and subcontractors are held liable under the HIPAA Security and Privacy rule. Cloud service providers that service companies in financial services or healthcare industries are also, in turn, impacted by those contractual and/or regulatory requirements.

Service providers can offer clients assurance through Service Organization Control (SOC) reports. These attestations focus on the design and operating effectiveness of controls related to financial reporting or operational controls at service organizations. SOC reports have become the market standard for third party attestation and can serve as a powerful testament to your company’s commitment to sound operating practices and the company’s ability to meet regulatory, compliance, and market demands. Increasingly, SOC is becoming a necessary prerequisite in order to advance in the sales discovery and RFP processes.

After completing this session, the participant will be able to:
- Know the difference between SOC 1, SOC 2, SOC 2+, and SOC 3 reports
- Be aware of the changes to the SOC standards,
- Describe the benefits of SOC reports, and
- Learn how to prepare for a SOC examination

IT Audit, Governance, Risk and Compliance (GRC)

G9 Cognitive Technology to Transform the Audit

Speaker **John Lee**
Director, Data & Analytics, KPMG

The buzz around cognitive computing, artificial intelligence, and deep learning have been enormous – tasks previously seen as human-only, such as chess, Jeopardy, Go! – are becoming dominated by intelligent algorithms with massive amounts of computing power. In industry, cognitive computing promises intelligent systems that can interact with customers, automate tasks, and learn to improve its performance over time. This market for cognitive solutions will grow rapidly over the coming decades, and fuel an estimated $1T automation industry. However, the road to tomorrow's success will rely on a firm understanding the evolution of cognitive, the different categories and applications for cognitive, and the factors that drive success in your company and transform your audit.

After completing this session the participants will be able to:

- Understand what cognitive means and the evolution of AI
- Distinguish between the different levels of cognitive automation with examples of each
- Understand the role of subject matter experts and process/knowledge experts in deploying cognitive automation
- Learn about the prerequisites to making cognitive solutions successful in your company

G10 Governing without clear standards: Lessons learned from the trenches

Speaker **Ron Raether**
Partner, Troutman Sanders, LLP

The term standard is used loosely in the context of data usage and security. While standard setting organizations work to provide guidance, the variables are too numerous such that a single, universal standard is not possible. What is emerging is not a standard, but instead a well developed process. It will ultimately be the use of this process, along with the rationale for the resulting decisions, which will determine whether a company acted commercially reasonable in building its compliance program. Collaboration among business, technologists, CISOs, CPOs, and attorneys will be essential to developing and maintaining a defensible program. Learn how existing standards and tools may not meet a regulator's or court's view of what is reasonable. From real world examples, you will learn how to develop a program which will stand up under scrutiny and what common pitfalls to avoid.

After completing this session the participants will be able to:

- Understand how the "standards" being offered by NIST, CSA, HHS, PCI, FFEIC may not offer legal standards for whether a company a company acted commercially reasonably.
- Understand views of the regulators and courts on standards
- Develop a program that nonetheless puts the company in the best position possible
- How to avoid common pitfalls
- What is considered good governance under the law

G11 Assurance with the NIST Cybersecurity Framework

Speaker **Nelson Gibbs**
First Vice President, East West Bank

Cybersecurity is one of the highest areas of concern for organizations today and one of the most difficult to effectively audit due to the increasing volume and sophistication of risk vectors and attacks as well as heightened legal and regulatory requirements, shareholder scrutiny, and the pace of technological change. Come to this session to get an in-depth look at ISACA's new Cybersecurity IS Audit/Assurance Program that can be used to perform an audit that is aligned with the NIST CSF and ISACA's COBIT 5 framework.

After completing this session the participants will be able to:
- Understand and apply the NIST CyberSecurity Framework based on COBIT principles and processes
- Identify security control concerns that could affect the reliability, accuracy, and security of enterprise data and systems
- Provide management with an assessment of their cybersecurity environment

G12 People Make the Best Exploits – For Security and Compliance Risks

Speaker **Jennifer Cheng**
Director of Solutions Marketing, Proofpoint

Digital disruption is creating new collaboration opportunities – but also spurring new security and compliance risks. The threat landscape will continually change but one fact remains the same: attacks always target people, because people are the weakest link in the cyber kill chain. People today are using email and mobile applications to communicate and do work. Do you have the visibility you need to understand how these tools are putting your organization at risk?

After completing this session, participants will be able to:
- learn about the evolution of targeted and advanced threats
- how to better protect your people, data, and brand from advanced threats and compliance risks

Women In Techology

W1 Story Telling: Effective Communication

Speaker **Kimo Kippen**
Vice President, Global Workforce Inititaives, Hilton Worldwide

When was the last time you retold a piece of information? Think about it. Was it something you heard from someone else? Was it something you heard from an online video or a news piece? Science tells us that recognition increases when we learn through stories. It further increases when we can use visuals over text and words. Our mind wants to explore all of the senses and when it does communication and what you learn through your communication experiences become part of you.

In this session, Kimo Kippen, CLO of Hilton Worldwide, will share with you a practical and conceptional presentation that teaches you how to build a story, how to tell a story, and how communication through stories can help you serve as a stronger leader, a more effective ambassador, and a more memorable citizen of the world. We will learn the essential pieces of a story and why those pieces will trigger parts of the mind to remember, recall and retell. Come prepared to share your own stories through the process you learn during our time together.

After completing this session, the participants will be able to:

- Understand how to build and tell a story
- Identify the critical components of a good story that will make it one that is remembered and retold
- Learn from sharing stories with others to practice the process

W2 Soft Skills for Assurance Professionals

Speaker **Shawna Flanders**
Director of Instructional Technology and Innovation, MIS Training Institute

This session will provide attendees with tips and techniques for effective oral and written communication. The course can also be expanded to cover topics in greater interest to the organization.

After completing this session, the participants will be able to:

- Understand communications basics including communications etiquette
- Understand effective Listening
- Learn the art of note taking
- Understand how to network effectively
- Learn how to sell your idea or conclusion verbally and in print

W3 Women In Technology Panel - The Path to Leadership

Speakers

Cheryl Santor
Information Security Manager, Retired from Metropolitan Water District of So. CA

Janice Pearson
Director, Content Protection, Warner Brothers Entertainment Inc.

Andrea Hoy
CEO, A. Hoy and Associates and President of Information Systems Security Association (ISSA)

How did you, or can you, achieve your position in the Technology realm? What steps, risks, initiatives did you incur along the path? How can your story get others involved with technology and provide more resources to the increasing number of candidates for the various technology fields. We are going to discuss those topics. Whether it be Information Security, Sciences, Critical Infrastructure, Engineering, Governance, Risk Management, Compliance, Audit. Find the technology arena you fit into and excel. Come and meet other individuals working to increase the level of women engagement and leadership in the technology fields.

After completing this session, the participants will be able to:

- Learn from hearing inspiring stories and ideas of success in the technical world and achieve benefits of what works
- Gather ideas and work toward achieving positions within the technology spaces
- Understand methods of entering technology, using interaction with peers, mentors, academics, wherever your exposure leads
- Learn how individuals have achieved and surmounted adversity, or struggles, or had a mentor to assist in achieving the positions they are in today
- Be interactive and engaged with leaders in technology

W4 Personal Branding

Speaker

Kimo Kippen
Vice President Global Workforce Inititaives, Hilton Worldwide

How you "show up" makes all the difference. Hilton works extremely hard on its presence as a company and has proven itself as a leader in its industry and as a Great Place to Work. But reputation and presence goes far beyond the company brand. The people who create that culture from within carry a responsibility too. Their personal brands are a reflection of the company they work for, the community they live and serve, and the family that surrounds them. In this session, former CLO and now VP of Global Workforce Initiatives, Kimo Kippen helps you to learn more about yourself through a branding lens. You will learn how to articulate the values and behaviors you demonstrate as part of your "whole person" and explore ways to present your best self.

After completing this session, the participants will be able to:

- Understand how to define and develop your own brand
- Explore the brands all around us and what they mean to us
- Manage your personal brand in a world of social media and instant gratification

Women In Techology

W5 Executive Presence

Speaker **Kristina Ridaoui**
Vice President- IT Audit, City National Bank

Executive presence is a blending of temperament, competencies, and skills that, when combined, send all the right signals. Leaders know they must embody executive presence to get ahead, influence others, and drive results. Leadership development professionals know they must help their executives develop it. Key traits include; emotional intelligence (IQ), self-development, strong executive functioning skills, etc.

After completing this session, the participants will be able to:

- Understand what is Executive Presence
- Understand the benefits
- Develop and refine Executive Presence

W6 Leadership – Building Collaborative Relationships to Drive Results

Speaker **Helen Norris**
Chief Information Officer, Chapman University

More than ever, leaders must collaborate with other groups in the organization to be effective. This is especially true for technology leaders, as technology initiatives touch every area of the organization. Learning to work in this more collaborative environment is critical to the success of CIOs, Information Security Officers and IT Auditors. The speaker will share her experiences building relationships and driving collaboration from the unique perspective of a female leader in a male-oriented profession. These lessons, while coming from the IT world, are applicable in all organizations.

After completing this session, participants will be able to:

- Build relationships across their organizations
- Deliver projects more effectively through collaboration
- Reduce friction in the organization

W7 So, You're Interested in A Career in Cybersecurity

Speakers

Patricia Benoit
Senior Manager, Cybersecurity & Compliance, Southern California Edison

Piunik Adamian
IT Specialist, Southern California Edison

If you are interested in a career in cybersecurity, this session will help you understand the areas that make up this exciting and growing field, and how to apply this information to your career plans. This session will help you understand key cybersecurity areas, how interests and experience align with each area, training options for expanding cybersecurity skills, and examples of cybersecurity career paths.

After completing this session, the participant will be able to:

- Identify the different areas of cybersecurity
- Identify interests and experience that aligns with each
- Identify types of training that supports expanding your skills into these areas
- Identify examples of plans for a career (or growing a career) in cybersecurity

W8 Inspiring Young Talent for Cyber Careers

Speaker

Lee Ann Kline
President & Founder, STEM Advantage

If she can see it, she can be it.” As IT professionals, you can be instrumental in developing the next generation of IT and cyber talent. As role models, mentors and by opening doors to internships, you can help develop women and other underserved communities, many of whom are first generation college students. They aspire to work for the FBI and Homeland Security. They are role models as well who want to address issues like cyberbullying. To succeed, they need support. STEM Advantage is a non-profit that developed a 360-degree program to provide women and underserved communities attending a public university – the California State University (CSU) – the type of support that many students attending a private university receive, including internships, mentors, scholarships, career panels, access to and networking opportunities with business and technology executives and hiring managers.

After completing this session, the participant will be able to:

- Understand why the younger generation is interested in “cyber”
- Learn how you and your employees can be role models and mentors to inspire young women and other underserved communities to pursue careers in IT and cybersecurity
- Learn about and how you can get involved with STEM Advantage, a non-profit organization that developed a 360-degree program to provide women and underserved communities attending a public university the type of support that many students attending a private university receive, including internships, mentors, scholarships, career panels, access to and networking opportunities with business and technology executives and hiring managers

W9 “I don't know how you do it." The Myth of Having it All

Speaker **Kim Lamoureux**
Manager, RiSK Opportunities

Working parents of today face different challenges from previous generations: a fast-paced work environment, the high cost of childcare, and dual-income households. For women in the workplace, the pressures of both excelling at work and at home can be overwhelming. We discuss realities of a working mom in the first years of childrearing and staying in the top of your field while navigating the unknown obstacles of being a parent.

After completing this session, the participant will be able to:

- Understand how to achieve personal and work goals without having to “have it all.”
- Understand how to achieve goals at work while balancing unpredictable family situations (sick children, traveling spouses, etc)
- Understand how to integrate technology and productivity tools to organize home and work life (Amazon, Evernote, Heal App, etc).
- Understand the realities of child care and how it affects the workplace
- Understand how to maintain a network of support
- Understand how to stay connected online and maintain privacy

W10 Topic: Mentoring the Next Generation: Finding and Developing the “Hidden Figures”

Speakers **Cora Carmody**
Former CIO, Jacobs Engineering

Nanxi Liu
CEO, Enplug

Major corporations, U.S. and worldwide, are still struggling with equal representation of women and minorities in Science, Technology, Engineering, and Math (STEM) careers. Major names in Silicon Valley, the coolest of the cool, have made public their own short fallings in this—tech companies often thought of as forward-thinking in a consumer-facing industry that is assumed to be more open and diverse than other companies. Yet recent disclosures at these tech companies have shown that their workforce is comprised of fewer than 20% of women in a technical role—and an even dramatically lower percentage of female executives and minorities in a technical role.

For over two decades, a tremendous amount of funding and attention has been directed to improve inclusion in STEM education and employment. Many of the well-known programs to help attract more females and minorities into technology and engineering degrees start at the high school level, occasionally at the intermediate level, and seldom at the early-mid elementary level. This session will engage you in a discussion of shared experiences and brainstorming around.

After completing this session, participants will be able to:

- Discuss what IS the right age for kids to dip their toes in the technology and engineering pool of learning?
- Understand what are methods that work?
- Determine who makes the best role models for encouraging STEM education?
- Understand In what ways should approaches be different for girls?
- Determine how can you or your company be more active in building the next generation of STEM-literate workers?

Women In Techology

W11 Recruiting Women for IT

Speaker

Anna Carlin
CIS Instructor, Fullerton College

Dan Manson
Professor, Cal Poly Pomona

Colleges perform outreach to middle, high school, and college-aged women to encourage them to major in IT related majors. School curriculum will be shared, extra curricular activities will be detailed, and opportunities for working professionals to become involved. We will also elaborate on the strengths and challenges when recruiting women.

After completing this session, the participant will be able to:

- Identify those schools recruiting and retaining women in IT related majors
- Identify the recruiting and retention methods used for middle school, high school, and college women in IT related majors.
- List how attendees can be involved in recruiting and retaining women into IT.

Sponsors

Gold Sponsors

www.sailpoint.com

SailPoint

SailPoint is the Worldwide Leader for Enterprise-Class IAM. We minimize risk and maximize business growth by managing access to data and resources across your enterprise. We do it effectively and securely for every person who interacts with your organization—any user, on any device, anywhere in the world. We were first to recognize that companies could benefit from an approach to identity that addresses both IT and business priorities. We developed a unique risk-based model and leveraged that approach for everything from compliance to user provisioning. Then we followed that with the industry's first solution for truly extending enterprise identity management to applications in the cloud. Today, we offer comprehensive products that can handle enterprise IAM on-premises or as a cloud-based service. This gives you the freedom to choose the best solution for your current needs, while at the same time establishing a clear path for future growth.

www.forcepoint.com

Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's behaviors and intent as they interact with critical data and IP wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to data while protecting intellectual property and simplifying compliance.

www.troutmansanders.com

Troutman Sanders LLP

Founded in 1897, Troutman Sanders LLP is an international law firm with more than 650 lawyers practicing in 16 offices located throughout the United States and Asia, including offices in San Francisco, Orange County and San Diego. The firm's clients range from large multinational corporations to individual entrepreneurs and reflect virtually every sector and industry. The firm's heritage of extensive experience, exceptional responsiveness and an unwavering commitment to service has resulted in strong, long-standing relationships with clients across the globe. In the technology sector, this experience spans a wide variety of issues and legal disciplines which includes knowledge of not just the law, but also a deep understanding of technology and emerging trends. In recognition of the firm's strong service culture, Troutman Sanders has been on the BTI Client Service A-Team for 13 consecutive years.

Sponsors

Silver Sponsors

www.disney.com

Disney

The mission of The Walt Disney Company is to be one of the world's leading producers and providers of entertainment and information. Using our portfolio of brands to differentiate our content, services and consumer products, we seek to develop the most creative, innovative and profitable entertainment experiences and related products in the world.

www.centrify.com

Centrify

Centrify is a leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. Centrify helps protect against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's apps and infrastructure for all its users.

www.symantec.com

Symantec

Symantec is the global leader in security. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Since its inception in 1982, Symantec has grown into a Fortune 500 company through a combination of internal development, strategic acquisition and partnering with industry leaders. Our award-winning solutions enable our customers to trust that their information and identities are secure independent of device or application.

www.grantthornton.com

Grant Thorton

Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. We help dynamic organizations grow by providing meaningful, actionable insights for privately owned, publicly listed and public sector clients.

Sponsors

Bronze Sponsors

www.cyberwatchwest.org

CyberWatch West

Located on the Whatcom Community College campus in Bellingham, Wash., CyberWatch West is the only NSF-ATE Center in the Western Region of the United States. Its work is supported by a National Science Foundation (NSF) Advanced Technological Education Grant. CyberWatch West is comprised of four leadership colleges and additional educational members and industry partners.

www.ey.com

E&Y

EY provides global services to help you retain the confidence of investors, manage your risk, strengthen your controls and achieve your potential. At EY, we are committed to building a better working world — with increased trust and confidence in business, sustainable growth, development of talent in all its forms, and greater collaboration. We want to build a better working world through our own actions and by engaging with like-minded organizations and individuals. This is our purpose — and why we exist as an organization. Running through our organization is a strong sense of obligation to serve a number of different stakeholders who count on us to deliver quality and excellence in everything we do. We want to use our global reach and scale to convene the conversation about the challenges facing economies and the capital markets. When business works better, the world works better.

www.kpmg.com

KPMG

KPMG operates as a global network of independent member firms offering audit, tax and advisory services; working closely with clients, helping them to mitigate risks and grasp opportunities. Member firms' clients include business corporations, governments and public sector agencies and not-for-profit organizations. They look to KPMG for a consistent standard of service based on high order professional capabilities, industry insight and local knowledge.

www.pwc.com

Pricewaterhouse Coopers

PwC focuses on audit and assurance, tax and consulting services. We help resolve complex issues and identify opportunities. With offices in 157 countries and more than 208,000 people, we are among the leading professional services networks in the world. We help organisations and individuals create the value they're looking for, by delivering quality in assurance, tax and advisory services.

Sponsors

www.reevert.com

Reevert, LLP

Reevert is a virtual backup appliance designed to provide seamless data protection and recovery from all forms of data loss, including ransomware and malware attacks. With local and cloud backup capabilities, it is the perfect, cost effective all-in-one backup solution. Along with full data and network share snapshots, it also supports image backups. With an easy to use web admin panel and built-in automation, it does all the work so you can focus on your business.

www.deloitte.com

Deloitte

The subsidiaries of Deloitte LLP provide industry-leading audit, consulting, tax, and advisory services to many of the world's most admired brands, including 80 percent of the Fortune 500 and more than 6,000 private and middle market companies. Our people work across more than 20 industry sectors with one purpose: to deliver measurable, lasting results. We help reinforce public trust in our capital markets, inspire clients to make their most challenging business decisions with confidence, and help lead the way toward a stronger economy and a healthy society. As part of the DTTL network of member firms, we are proud to be associated with the largest global professional services network, serving our clients in the markets that are most important to them.

Total Visibility. Focused Protection.™

www.skyboxsecurity.com

Skybox Security

Skybox Security arms enterprises with a powerful set of security management solutions that give unprecedented visibility of the attack surface and key indicators of exposure. Our solutions unify data by integrating with 90+ security technologies. With analytics, modeling and simulation, Skybox provides security pros the insight needed to quickly prioritize and address vulnerabilities and threat exposures in the context of the business environment, increasing operational efficiency by as much as 90 percent.

www.trendmicro.com

Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection.

With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Find Us on Social Media

facebook.com/ISACALA.ORG

twitter.com/isacala

linkedin.com/groups/1991652

global conferences
membership
certifications
knowledge
training
education
career management