Learn the implications of cyber security.

In today’s society, technology is embedded in everyone’s life. How secure is your home, your business and your identity? Do you want to understand what it means to be secure in “the cloud,” safeguard your assets and keep your confidential files away from hackers?

At the University of Phoenix Technology Conference, you will be provided with the tools to understand cyber security, learn best practices to secure the Internet of Things, and discuss the implications of cyber security on you and your community.

• Meet experts in the fields of cloud security, digital forensics, identity-theft prevention and protection, cyber espionage and threat research.
• Learn from a panel of speakers about the U.S. military’s and law enforcement’s war against cyber-attacks.
• Attend workshops and breakout sessions on topics such as securing social media, how should you use free Wi-Fi, how viable is your big data and more.

This event is open to anyone interested in learning about cyber security, and how to protect one’s homes, businesses, and assets.
Table of Contents

Agenda 0
Vendor Showcase 4
Keynote speaker 13
Lunch & Learn / Meet & Greet 14
Presenters 21
Topics / Presentations 23
Conference Schedule 34
Special Thanks 41

Agenda

8:00 to 9:00 am
Registration and Breakfast
Lobby & Room 105
Vendor/Presenter Check-in
Room 104

9:00 am
Welcome Remarks
Room: 106-107

9:15 am
Keynote Speaker
Room: 106-107

10:15 to 11:00 am
Session I
See schedule for details

11:30 to 1:00 pm
Lunch ‘n’ learn
Room: 106-107

1:15 to 2:00 pm
Session II
See schedule for details

2:15 to 3:00 pm
Session III
See schedule for details

3:15 to 4:00 pm
Session IV
See schedule for details
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills.

CyberTECH
Global cybersecurity and Internet of Things (IoT) network ecosystem providing cybersecurity and IoT resources, strategic programs and thought leadership events across the nation. In partnership with national and local organizations, the CyberTECH mission is to stimulate innovation and advance the adoption of cyber and IoT technologies for the economic and social benefit of the nation. We accomplish this through a series of programs and leadership opportunities.

Our membership includes business and financial leaders, academic and research institutions, government and non-profit organizations.

http://cybertechnetwork.org/

Federal Bureau of Investigation (FBI)
Our Mission
As an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

Our people in San Diego possess a mix of talents and experience that enable us to help protect you, your families, and your workplaces from a full range of national security threats and major crime problems.

Our employees are not only special agents, but also a variety of specialized professionals such as intelligence and financial analysts, investigative specialists, support services technicians, language specialists, paralegals, electronics technicians, and security experts.

http://www.fbi.gov/sandiego

Special Agent Angela R. Winn, HR Recruiter for the FBI will be available to meet guests with IT Security background to discuss opportunities with the FBI.
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

San Diego District Attorney’s Office

Mission: The employees of the San Diego District Attorney, in partnership with the Community we serve, are dedicated to the pursuit of truth, justice, and protection of the innocent and the prevention of crime through the vigorous and professional prosecution of those who violate the law.

Our Bureau of Investigation is comprised of approximately 158 investigators. We have 113 District Attorney Investigators. Their law enforcement authority comes from the same section of the penal code, 830.1, as a deputy sheriff or city police officer. What is unique about our law enforcement team is that they come to us from other law enforcement agencies. Most come from our local law enforcement agencies but we have several who have come from state and federal agencies. They have all completed the basic POST academy, and are required to meet the ongoing training requirements set forth by POST.

Once hired, many of our District Attorney Investigators will be assigned to areas that they have experience in, such as pre-trial support, gangs, robbery, narcotics, homicide, and family protection (which includes domestic/child/elder abuse and child abduction). Along with these areas, we have an increasing number of investigators who work in specialized units such as computer and high tech crime, environmental, real estate, consumer, and workers compensation fraud. We also have investigators assigned to the areas of public integrity, Mexican Liaison, backgrounds, officer involved shootings, and internal affairs. We provide extensive training and mentoring in order to assist our investigators as they transition into these very complex, technical and specialized investigations.

http://www.sdcda.org/

San Diego Digital Forensics

Our forensic expert consultants have all had Secret or Top Secret clearances for their employment with their government agencies. Our consultants are truly trained to "government standards." Training has include courses conducted by: the US Department of the Treasury; the Department of Homeland Security, Immigration and Customs Enforcement (ICE); Federal Bureau of Investigations (FBI), FBI Computer Analysis Response Team (CART); FBI National Infrastructure Protection Center (FBI NIPC); US Department of Defense; National White Collar Crime Center; SEARCH, The National Consortium for Justice Information and Statistics; and the International Association of Computer Investigative Specialists.

http://sd-df.com/index.html
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

San Diego Police Department
Mission: To maintain peace and order by providing the highest quality police services.

The San Diego Police Department offers a variety of resources related to crime prevention and education, including crime statistics and maps, neighborhood division maps, as well as instructions on reporting emergencies and non-emergencies. In addition, listings of San Diego Police Department units and other law enforcement-related agencies and organizations are provided along with useful resources.


Chula Vista Police Department
Chief Bejarano leads a department of 225 sworn officers, 90 civilian employees, and more than a hundred volunteers (Organizational Chart). The department maintains a budget of just under $50 million and provides law enforcement services to a community of over 250,000 people. Chula Vista is the second largest city in San Diego County, 13th largest in the state and the 89th largest in the country. Chula Vista was recently designated the 10th safest city in the United States for jurisdictions with more than 200,000 population.

http://www.chulavistaca.gov/departments/police-department

City of San Diego
Cybersecurity Awareness needs continuous attention by everyone, not just one month a year. Key areas of concern nationally are identity theft and protecting children in their use of the Internet and Email. The purpose of the City of San Diego’s Cybersecurity Awareness effort is to educate citizens and its employees about the potential dangers of using the Internet and Email, and the simple steps that can be taken to help protect yourself personally, as well as our local businesses and City government from cyber-attacks, fraud, identity theft, and other malicious activities.

You are encouraged to learn more about cybersecurity by checking the available cybersecurity resources.

Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

FireEye

A leader in providing cyber security solutions, protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive Incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you’ll detect cyber-attacks as they happen, understand the risk they pose to your most valued assets, and have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,500 customers across 65 countries, including over 150 of the Fortune 500.

https://www.fireeye.com

Stella Coulson, HR Recruiter for FireEye will be available to meet guests with IT Security background to discuss opportunities with FireEye.

KPMG

KPMG provides audit, tax and advisory services and industry insight to help organizations negotiate risks and perform in the dynamic and challenging environments in which they do business.

Our experienced IT security partners and professionals possess leading technical expertise, and are some of the most highly regarded in their specialties.

We have extensive experience building, delivering and supporting cybersecurity programs for Fortune 500 and Global 2000 companies across a multitude of industries.

We tap into the expansive services portfolio of KPMG’s global network to bring clients cross-functional knowledge and resources to support complete IT security transformations.


Engility

Engility’s Business strategy is based on an economic model that provides precisely the services needed at the best possible cost. Our portfolio of offerings reflects a lifecycle of capabilities that aligns with the critical priorities of the U.S. Government, both domestically and globally as well as state and local governments.

http://www.engilitycorp.com/
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

Department of Justice
United States Attorney’s Office
Southern District of California

Cybercrime is one of the greatest threats facing our country, and has enormous implications for our national security, economic prosperity, and public safety. Attorney General Eric Holder has made it one of the Department of Justice's top priorities. The range of threats and the challenges they present for law enforcement expand just as rapidly as technology evolves.


Cyber Center of Excellence

Founded by a collection of world-class cyber companies with operations in San Diego, the CCOE is open to any organization with a stake in our regional economy. Early participants include Sentek Global, ESET, General Dynamics, Qualcomm, Sempra, FICO, Lockton Insurance, Morrison Foerster and the United States Navy’s Space and Naval Warfare Systems Command (SPAWAR).

• Fostering cooperation throughout the established cyber community
• Attracting and nurturing talent
• Creating new opportunities for business

http://sdccoe.org/

San Diego County Sheriff’s Department
The San Diego County Sheriff’s Department is the chief law enforcement agency in San Diego County. The department is comprised of approximately 4,000 employees, both sworn officers and professional support staff. The department provides general law enforcement, detention and court services for the people of San Diego County in a service area of approximately 4,200 square miles. In addition, the department provides specialized regional services to the entire county, including the incorporated cities and the unincorporated areas of the county.

http://www.sdsdsheriff.net/
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

redIT
Best-In-Class Enterprise Level Data Center Services
We engineered our facilities to deliver world-class reliability while offering a flexible, customizable suite of data center options. Our experienced team is dedicated to helping you implement the solution that your business requires, no matter how unique it may be.

http://us.redit.com/

HR Recruiter for redIT will be available to meet guests with IT Security background to discuss opportunities with redIT.

LP3-SecurIT
A well-established provider of cyber security, compliance, infrastructure and incident response services to organizations across the USA.
We’re celebrating 10 years of protecting the nation’s most valuable networks and infrastructure. Our ‘First Decade of Defense’ as a company.

With every engagement, we focus on your unique challenges and ensure that the right people and the right solutions are applied effectively to meet your needs...

http://www.chulavistaca.gov/departments/police-department

Protecting Tomorrow
“Protecting Tomorrow by Taking Action
Those of us in Protecting Tomorrow fully understand a change has to come to our country. We fully believe that we, as individuals and as a group, can truly make an impact -- together we can make a difference. Bring your own passion and help make a difference in our nation -- help protect all of our tomorrows.

We have to make a change -- we have to do something differently for us to survive as a nation

- Our children are dying in our schools
- Our SMBs are being devastated by cyber attacks
- Our emerging technologies are moving off shore and are emerging without cyber protection built-in
- Our transitioning vets are living on the streets or committing suicide in record numbers.

https://protectingtomorrow.org/
Vendor Showcase

Meet our fabulous partners, joining forces to help prevent cyber-attacks, educate communities, and build awareness of potential threats, and supporting on-going collaboration and increasing skills

McAfee
McAfee, part of Intel Security, is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and businesses of all sizes from the latest malware and emerging online threats. Our solutions are designed to work together, integrating antimalware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve Internet security, and help businesses achieve operational efficiencies

McAfee Security
Backed by an award-winning research team, McAfee security technologies use a unique, predictive capability that is powered by McAfee Global Threat Intelligence — enabling home users and businesses to stay one-step ahead of online threats.

http://www.mcafee.com/us/

TestOut
TestOut is the leader in online labs for academia and IT professionals. With LabSim, students get a broad range of hands-on experience in a safe, simulated environment. Since our founding in 1991, we have helped hundreds of thousands of individuals acquire the skills they need to progress in their education and careers.

http://www.testout.com/

Fedcom Technology
Fedcom Technology is an IT company dedicated to providing IT services to small medium businesses in San Diego.

Fedcom Technology has successfully implemented IT solutions & Services to life science organizations, Finance, Accounting, Engineering Firms, Architectural firms, Legal firms and many more industries; our services include but not limited to Desktop Support, Server Support, Network Support, and Backup & Recovery.

http://www.fedcomtechnology.com/
Welcome and remarks

Dennis Bonilla
University of Phoenix

As executive dean, Dennis is responsible for all aspects of the College of Information Systems and Technology, including the college’s financial and academic performance and its marketing and operations. Dennis’ wealth of experience in delivering technology leadership and innovation spans a variety of industries, including education, telecommunications, energy, and nuclear engineering. Prior to joining University of Phoenix, Dennis was senior vice president of learning solutions at GP Strategies Corp., where he kept charge of global account strategy for Microsoft and other Fortune 500 companies.

Keynote Speaker

RADM (Retired) Kenneth D. Slaght
Center of Excellence

RADM Kenneth D. Slaght, USN (ret.) is the Co-Chair and President of the San Diego Cyber Center of Excellence (CCOE), which is a public-private partnership established to coordinate and enhance the effectiveness and synergy of the regional cyber initiative, capitalizing on our unique strengths to accelerate the regional economy by creating opportunities for business, attracting, and nurturing talent.

Previously, RADM Slaght served as the Vice President and General Manager, Navy/Marine Corps Services Sector, General Dynamics Information Technology, responsible for providing IT services to the Navy and Marine Corps. Prior to that, he was the Commander of the Space and Naval Warfare Systems Command. He was responsible for providing information technology and space systems for naval and joint services. Additionally, he was the chief engineer for developing, delivering and maintaining effective, capable, and integrated command, control, communications, computer, and intelligence systems (C4I). He was also responsible for engineering and assessing FORCEnet, the foundation of the Seapower 21 vision.

During his naval career, RADM Slaght served as Commander of the ammunition ship USS FLINT (AE 32). Other sea duty included tours as Executive Officer aboard the guided missile cruiser USS GRIDLEY (CG 21), Engineer Officer aboard the amphibious ship USS TULARE (LKA 112), Operations Officer aboard the frigate USS EDWARD MCDONNELL (FF 1043), and Combat Information Center Officer aboard the frigate USS GARCIA (FF 1040).

RADM Slaght received his commission in 1970 upon graduation from the United States Naval Academy. RADM Slaght attended the Defense Systems Management College, the Naval Post Graduate School, where he received a Master’s Degree in Computer Systems Management, and the Naval Destroyer School. He currently serves on the Boards of the National Defense Industrial Association (NDIA), the San Diego Military Advisory Council (SDMAC), the San Diego State University Industry Advisory Board, and the Point Loma Nazarene Business School Advisory Board.
Rusty Sargent, CFCE

San Diego Digital Forensics

Rusty Sargent started his law enforcement career with the La Mesa California Police Department in 1980. Mr. Sargent worked Patrol, started the Department’s K-9 Unit, worked in the Traffic Division, and was a Detective in the Investigations Division.

As a detective, he investigated cases including homicide, robbery, violent crimes, sex crime, child abuse, missing persons, fraud and forgery, burglary and thefts. In 1989, Mr. Sargent started the department’s high tech crime unit, working all computer related crimes, any crime involving a computer, and conducting computer forensics investigations.

In 1998, Mr. Sargent was involved in the formation of the first Regional Computer Forensics Laboratory (RCFL) in the United States, based in San Diego. In 2000, Mr. Sargent along with several other examiners with San Diego RCFL, had several meeting with Attorney General Janet Reno, and as a result, the San Diego RCFL was adopted by the US Department of Justice and became the role model for the FBI’s RCFL National Program. Mr. Sargent was a Senior Examiner, Team Leader, and in 2002 became the Operations Manager of the San Diego RCFL supervising the day-to-day operations of the RCFL and that of 20 law enforcement personnel. While at the RCFL, Mr. Sargent was cross sworn as an FBI Special Officer and as a Deputy U.S. Marshall. Mr. Sargent also held a Top Secret SCI clearance while in government service.

Mr. Sargent retired from law enforcement in August 2004 and worked for several Computer Forensics and Electronic Discovery companies, both small and large, as a Senior Examiner, Manager, Regional Practice Leader, and Vice President of Computer Evidence, handling computer forensics, electronic discovery, litigation support and client management for civil litigation matters. In 2009, Mr. Sargent formed his own computer forensic company, Sargent Digital Forensics, Inc., providing computer forensics and electronic discovery services for civil litigation matters. In 2013, the industry experienced tremendous growth, and as a result, in 2014, he partnered with Jim Sevel and Don Evans of San Diego Computer Forensics, LLP to form San Diego Digital Forensics, Inc.

Mr. Sargent has been a member of and involved in the International Association of Computer Investigative Specialist (IACIS) since 1999. He received his Certified Forensic Computer Examiner (CFCE) certification in 2002 and immediately started coaching/instructing law enforcement investigators through their certification process for their CFCE certification. Mr. Sargent has been an instructor for the IACIS International yearly training conference teaching computer forensics to local, state, federal, and international law enforcement officers since 2004. He has maintained his CFCE certification, renewing it in 2005, 2008, 2011, and again in 2014.
**Lunch & Learn Panel / Meet & Greet**

**Brendan McHugh, DDA**
*San Diego District Attorney’s Office*

Brendan McHugh has been a Deputy District Attorney with the San Diego County District Attorney’s Office since 2007. Brendan was previously a Deputy District Attorney with the Riverside County District Attorney’s Office, and prior to that worked for ten years in engineering as an engineering technician and associate engineer on cell phone base stations and consumer electronics. Brendan currently serves as the Project Director for the Computer and Technology High Tech Crime Response Team (CATCH), which encompasses San Diego, Riverside, and Imperial Counties. CATCH is a multi-agency task force comprised of Federal, State and Local law enforcement that investigates and prosecutes individuals involved in high tech crime.

**Sergeant Mark Varnau**
*San Diego County Sheriff’s Department*

In this high-tech age, cybercrime is a growing concern for people around the globe. During the holidays, millions of Target shoppers across the United States had their credit/debit card information compromised by hackers.

Recently, Sheriff's Sgt. Mark Varnau with the Computer and Technology Crime High Tech Response Team (CATCH) was a guest on KUSI News’ "San Diego People" program to discuss cybercrime in depth. Watch this video to learn how to protect yourself from becoming a victim of cybercrime.

To report any identity theft, internet or financial crimes, call the Sheriff's Department at (858) 565-5200. To learn more about the Financial Crimes Unit, visit: sdsheriff.net/financial/.

**AUSA Sabrina Feve**
*Assistant United States Attorney in the Southern District of California*

Sabrina Feve is an Assistant United States Attorney in the Southern District of California where she is assigned to the National Security and Cybercrime Section. Sabrina has served as the Computer Hacking and Intellectual Property Coordinator and the Identity Theft Coordinator since 2011. Prior to joining the San Diego U.S. Attorney’s Office, Sabrina practiced employment law and commercial litigation in San Francisco.
Mandy Griffith is an Assistant United States Attorney in the Southern District of California. After graduating cum laude from Baylor Law School, she worked for two federal judges and worked with a large Dallas law firm practicing employment law. Ms. Griffith worked in the Dallas County District Attorney’s Office from 2003 to 2009. She was assigned to the Child Abuse Division for over two and a half years and prosecuted cases involving child physical and sexual abuse. Ms. Griffith joined the United States Attorney’s Office in the Eastern District of Texas in 2009 where she worked as the Project Safe Childhood Coordinator prosecuting cases involving child sexual exploitation. Additionally, she served as the point-of-contact for human trafficking investigations and prosecutions for the district. In July 2014, Ms. Griffith transferred to the Southern District of California. Since joining the Southern District of California, Ms. Griffith has worked on a variety of cases and has continued working cases involving child sexual exploitation and human trafficking. As of May 2015, Ms. Griffith also serves as the Civil Rights Coordinator for the district.

Craig Rosen

FireEye

In his role as the Vice President and Chief Security Officer at FireEye, Craig is broadly accountable for providing transparent and protective security and risk management services that enable FireEye to maintain industry-leading levels of product and service assurance and customer trust. Craig’s leadership approach is centered on strategic business enablement through development of a data-driven and risk-aware culture, and he has a passion for building robust and resilient security architectures.

Craig is a technologist at heart and is enamored with the challenges of not only solving complex problems, but also communicating and driving them to completion with simplicity. Prior to FireEye, Craig served as the Director of Technology Risk & Strategy at Pacific Gas and Electric Company (PG&E). In that role, Craig was accountable for embedding technology risk management, measurement, and mitigation across every line of business, as well as the authorship and delivery of the company’s internal and publicly-facing enterprise security strategy. Craig also served as the Chief Security Architect at PG&E and launched the first enterprise security architecture practice at the company. Before joining PG&E, Craig consulted for large clients in both the public and private sectors in the Washington, DC metro area. Craig has been practicing and consulting in the field of information technology and security for over 18 years and holds a Master’s degree in Information Systems Technology from George Washington University, and a Bachelor’s degree in Economics and Law & Society from American University. Craig holds multiple security certifications, including the CISSP, ISSAP, ISSMP, and CRISC.
Lunch & Learn Panel / Meet & Greet

Supervisory Special Agent Terry Reed
Federal Bureau of Investigation (FBI), San Diego
Supervisory Special Agent and Cyber Program Coordinator

SSA Terry Reed leads FBI San Diego’s efforts to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. These high-profile cases focus on criminals who are invading countless homes and offices across the nation by breaking into laptops, personal computers, and wireless devices via hacks and bits of malicious code. Many of these cases have national security implications.

SSA Reed has held leadership positions at FBI headquarters and had a tour of duty in Athens, Greece as part of the FBI’s Legal Attaché program, which provides for a prompt and continuous exchange of information with foreign law enforcement and security agencies that have jurisdiction over the matters under investigation. As a Special Agent, SSA Reed led several successful Public Corruption investigations, which were featured in documentaries on PBS Frontline and CBS News Sunday Morning, among others.

Prior to joining the FBI in 2004, SSA Reed was a Senior Manager at Ernst & Young where he led large-scale, global system integration projects for Fortune 500 companies. SSA Reed holds a bachelor’s degree in Operations Management from the University of Minnesota.

Special Agent Jason Pearson
Federal Bureau of Investigation (FBI), San Diego

Jason Pearson is a Special Agent assigned to the San Diego Division of the Federal Bureau of Investigation (FBI). Prior to joining the FBI, Mr. Pearson formed an information technology firm out of Chicago, Illinois. As proprietor of the company, Mr. Pearson led a variety of IT security investigations and worked as a network and systems engineer for the healthcare, legal, and financial industries.

In 2009, Mr. Pearson joined the FBI and was assigned to the bureau’s Cyber Squad and High Tech Crimes Task Force, where he currently investigates Criminal Cyber Crime offenses.

Mr. Pearson is currently on the front line of investigations involving some of the largest and most complex financial fraud schemes to date and has assisted on a number of investigations involving Counter Intelligence and Domestic Terrorism matters. Mr. Pearson’s expertise involves the use of sophisticated Botnets and Malware, Computer Intrusion matters, and Automated Clearing House (ACH) fraud.
Shirley Adams is the Executive Director for CyberTECH, the nation’s leading cybersecurity and Internet of Things (IoT) business network. Most recently, Shirley was President, SPAWAR Services, GDIT Navy/Air Force Services Sector. She is a seasoned executive with over twenty years’ experience delivering on-target action strategies for small and large organizations.

Her leadership history with major businesses such as GDIT, Systems Engineering Solutions (SESI) and Mazda; providing IT services for large firms such as Boeing, Airbus, Pratt & Whitney, their OEMs, Dealership Franchises, and the Department of Defense, have resulted in major team productivity improvements, achievement of multimillion-dollar milestones, and successful new profit-center launches. As a strategist for revenue growth and business management, Ms. Adams has counseled companies to industry leader positions by helping them broaden market share and increase profits. Her passion for getting the job done and her lead by example attitude sets her apart as being a leader of heart and strength.

As an accomplished leader, teacher, author, and speaker, she has been recognized by all segments of the business community and is the recipient of numerous awards from both industry and government including:

- Crystal Airplane Award - Development of Innovative Solutions in the Commercial Aerospace Industry
- Top Influencials Award - San Diego Daily Transcript
- “Women Who Mean Business” Award - San Diego Business Journal
- Strathmore’s Who’s Who - Lifetime Honoree
- Excellence in Leadership Award, AFCEA International

She has an uncanny ability to hone in on the underlying issues and deliver practical and insightful solutions that have immediate impact on cash flow, profitability, and success.

Shirley is also involved with various professional organizations and industry associations, including the Air Transport Association (ATA) as a working group member for the development of world-wide commercial standards and specifications, the National Defense and Industrial Association (NDIA); former Chairman of the Board, and the Armed Forces Communications and Electronics Association (AFCEA); current AFCEA International Regional Vice President for the South Western Region and Past President for the San Diego Chapter. She also serves on the Board of Advisors for FleetWeek San Diego, an organization honoring our military.

Ms. Adams is a graduate of Northwood University with a Bachelor’s degree in Marketing and Business Management and is a resident of San Diego, California.
Lunch & Learn Panel / Meet & Greet

Captain Lon Turner
Chula Vista Police Department

Captain Lon Turner began his volunteer service with the police department in 1984 as a police explorer and later a reserve officer. In 1990, he was hired as a State Traffic Officer by the California Highway Patrol. In July 1991, Captain Turner rejoined the police department as a regular sworn officer. He served as a field-training officer, mobile field force member, narcotics detective, and task force agent. He received civic and department awards for "Officer of the Year," auto theft, proactive narcotics arrests, and lifesaving. In 1997, he was nominated for "Narc of the Year" with the California Narcotic Officers' Association (CNOA). In 2000, he was promoted to sergeant and served as a patrol supervisor and Special Investigations Unit supervisor. He was promoted to police lieutenant in 2004. As a police lieutenant, he served as a Watch Commander, Jail manager, acting Crime Lab manager, Professional Standards Unit manager, and Investigations lieutenant. In 2013, he was promoted to Captain, and currently leads the Investigations Division.

Captain Turner received his Associate's Degree from Southwestern Community College. He holds a Bachelor's Degree (Cum Laude) in Criminal Justice and Master's Degree in Public Administration from National University.

Captain Turner is a graduate of POST Command College (Class 49) and received the peer nominated "Hank E. Kohen" award for "most inspirational" student in 2011. He is a graduate of the Los Angeles Police Department Leadership Program and Drug Enforcement Administration's Drug Unit Commanders Academy (Class 71). He is a lifetime member of the CNOA, a published author, and part-time adjunct community college instructor.

David O’Berry
McAfee, part of Intel Security Company

David O’Berry is a "reformed CxO/CIO currently working for 'The Dark Side' in Worldwide Strategic Technologies within McAfee’s Office of the CTO." He spent 19 years on the enterprise side as a network manager, Director of Information Technology Systems and Services and, most recently, Director of Strategic Development and Information Technology in the public sector. During that timeframe, he was an advocate for standards-based networks and security working with groups like Trusted Computing Group and The Open Group to further those causes. Active within the industry, he currently holds CISSP-ISSAP, ISSMP, CISSLP, CRMP, among other certifications including old school certs like Master Certified Novell Engineer (a fact he tries not to mention very often). He has also been published several years in a row in the Information Security Management Handbook around standards-based distributed network visibility and autonomic security concepts as well as writing for various publications over the years on a wide-range of IT and IT-SEC topics. He calls himself a professional mutt because his background and experiences have been anything but a planned path throughout his career. Most recently, he was honored as a ComputerWorld Top 100 IT Leader for 2011, a fact he attributes to the amazing team that surrounded him during his service in the public sector.
Matt Stamper, MPIA, MS, CISA, ITIL, CIPP-US
redIT

Matt Stamper serves on the Board of Directors and is the Vice President of Managed and Professional Services at redIT, where he oversees the design and development of the company’s cloud-based managed services and security solutions including the implementation of redIT’s Hybrid Cloud Service Integration capabilities with Global Services Providers such as Amazon Web Services (AWS).

As a Certified Information Systems Auditor (CISA) with extensive public-company experience, Matt brings a depth of understanding of IT best practices, managed-services technologies, and compliance requirements to redIT’s clients.

Prior to joining redIT, Matt served as Vice President of Development for CFO Strategies, leading the development of the company’s IT governance software for Sarbanes-Oxley compliance and risk-management. As part of his work with CFO Strategies, Matt provided advisory services to public companies supporting both domestic and international engagements including projects in China. Prior to CFO Strategies, Matt worked in the managed services industry helping firms design highly-available and highly-resilient application architectures. Matt previously was a District Manager with VeriCenter (now SunGard); the Western Region Solutions Manager for AT&T’s Enterprise Hosting Division; Vice President of Business Development for Front Porch, Inc.; and an International Account Executive for AT&T’s Global Services Division. Matt’s executive-level experience with data centers, security services, and IT services provides a unique and broad perspective on the fast-changing world of enterprise IT.

Matt currently serves as president of the board of directors for the San Diego Chapter of the Information Systems Audit and Control Association (ISACA) and co-chair of the Telecommunications Sector for the San Diego InfraGard chapter. Matt is on the Board of Advisors for CyberFlow Analytics, the Board of Advisors of CyberTECH San Diego, an instructor on Cloud Security and Governance for UC San Diego’s Extension Program, ITIL Foundation certified, and a frequent speaker at IT-focused events.

Matt received a Bachelor of Arts from the University of California at San Diego, where he graduated Cum Laude and with Honors and Distinction in Political Science. Matt’s graduate studies include a Master of Arts in Pacific International Affairs from the University of California at San Diego and a Master of Science degree in Telecommunications sponsored by AT&T. Matt is fluent in Spanish.
Meet our Incredible Presenters

Gary Hayslip
City of San Diego

As Chief Information Security Officer (CISO) for the City of San Diego, Gary advises the City of San Diego’s executive leadership consisting of Mayoral, City Council, and 40+ city departments and agencies on protecting city government information resources.

Gary oversees citywide cyber security strategy and the enterprise cyber security program, operations, compliance and risk assessment services. His mission includes creating a “risk aware” culture that places high value on securing city information resources and protecting personal information entrusted to the City of San Diego.

Gary is involved in the cybersecurity and technology start-up community in San Diego where he is the Co-Chairman for Cybertech, the parent organization that houses the Cyber incubator Cyberhive and the Internet of Things incubator iHive. He also serves on the board of Brier & Thorn International; a cloud based Managed Security Services Company.

He is an active member of ISSA, ISACA, OWASP, INFRAGARD, and holds numerous professional certifications including CISSP, CISA, and CRISC. He holds a BS in Information Systems Management, Masters in Business Administration, and has over 25 years of experience in Information Security, Enterprise Risk Management, and Threat Mitigation.

LinkedIn Profile: [http://www.linkedin.com/in/ghayslip](http://www.linkedin.com/in/ghayslip)  Twitter: @ghayslip

Dean Larsen II
KPMG

Dean Larsen is a Manager with KPMG LLP’s Forensic Advisory Services practice where he is a member of the Forensic Technology Services group focused on Information Governance and Cyber Risk Management. Mr. Larsen has over twenty years of experience in global IT project execution and client service delivery for technology process improvements. He began his career with application development, moving to database administration, capacity planning, performance tuning and moved to unstructured content management.

He has advised on deploying enterprise content management solutions, data modeling, database applications, data analytics, mobile computing, cloud computing strategies, cyber security, and records management. Mr. Larsen has architected solutions from cloud-based computing infrastructures to mainframe data centers to distributed network server environments. Mr. Larsen serves as a subject matter professional expert for a broad spectrum of technology on multiple platforms. He has assisted clients in energy, financial services, manufacturing, healthcare, public sector, biotech and technology respond to challenges in security, business processes and implementing electronic stored information solutions. Prior to joining KPMG, Mr. Larsen spent over sixteen years at IBM in numerous roles including the IBM Consulting Group, Channels, and the Software Group in an international capacity. He recently led the deployment for 1.3M user system loading a half a million content objects the first week.
Meet our Incredible Presenters

Joe Lodewyck
University of Phoenix

Joe Lodewyck is the associate dean of assessment for the College of Information Systems and Technology. He has been an Oracle database designer and developer for more than 20 years. Throughout his career, Joe has worked on many database applications in a variety of business environments, including an obstetrical database application used for research, two student information systems, and applications supporting the facilities management for a large oil company. He most recently worked in the Office of the Provost as the director of academic data, leveraging both his technical and academic backgrounds to support, consult on, and interpret the technical and data needs of the various schools and college of the university.

Dr. John Sahlin
Engility

Dr. John Sahlin is the Technical Director of Information dominance for the Engility Corporation, driving the strategy and vision to apply commercial technology and best practices to the U.S. Department of Defense. His previous posts within the Public Sector include being the Chief Engineer for PMW 160’s SCN, OCF, and CANES Future program and the Chief Technology Architect for the County of San Diego. Dr. Sahlin is a leading technical expert in the fields of Systems Engineering, distributed computing network design, and managed hosting services. He has over 20 years’ experience designing, building, and sustaining distributed computing networks for commercial and U.S. Public Sector clients, applying his expertise in the ASP and Cloud Computing industries to the government sector. Dr. Sahlin holds a PhD in Systems Engineering from the George Washington University. He is currently an Adjunct professor at both the George Washington University and Coleman University. His current research is the subject of an upcoming textbook on alternate uses of social media.

Brandon Kravitz
Jungo

Brandon Kravitz is a local San Diegan developer and technology enthusiast. Receiving an award from Cisco & GTE for web technology at the age of 11, Kravitz always knew he wanted to be in technology. Kravitz has research interests in Software Defined Radio, application security, secure software design in the cloud and cybercrime. He has worked on a number of projects pertaining to penetration testing and forensics for small companies around North County San Diego. He is an avid participant in BlackHat, San Diego Toorcon, DEFCON, RSA and OWASP as well as an avid disc golfer.
Meet our Incredible Presenters

Dr. Richard Swafford, MBA, MaEd, MIS, MC/MFT, MSAJS, MHA, PhD

*Orion Health Inc.*

Dr. Swafford has over 30 years of experience in the information technology (IT) industry with specialized experience in education and health care information technology (HIT).

His proven leadership in not only the day-to-day activities of an IT organization but the ongoing strategic planning efforts associated with a variety of industries, is represented by his ability to leverage the most positive attributes from his staff while maintaining a level of professionalism that creates confidence in customers and end users. His holistic approach to technology implementation and management is evident in the various successes experienced throughout his career.

Leveraging his experience in the Health Information Exchange (HIE) space, Dr. Swafford provides consulting and solution architecture support to Orion Health’s current and future customers. He is focused primarily on the business aspects of creating and operating an HIE including strategic and financial modelling associated with both public and enterprise HIE deployments.

Prior to joining Orion Health, Dr. Swafford was the Executive Director for the Inland Empire Health Information Exchange (IEHIE). Dr. Swafford worked with a collaborative governance team to build and deploy a multi-state, multi-facility HIE environment that provided services in 7 states with more than 9 million patients and over 150 participating facilities.

Dr. Swafford helped to launch the California Health Information Partnership and Services Organization (CalHIPSO), the California State Regional Extension Center (REC) as the Chief Technology Officer (CTO). His involvement in the development and deployment of the REC service delivery model, vendor contract negotiation (Group Purchasing Contracts) and management of service partners led to the successful rollout of the REC for the state.

As the Chief Information Officer (CIO) of the Community Clinics Health Network (CCHN), Dr. Swafford was responsible for the Technical Services Organization (TSO). This department focused on technical solutions for its members in the form of consulting, planning, hosting, application and system support, training and product selection/implementation.

Dr. Swafford is presently a member of the faculty for a number of large Universities in Southern California. His education has allowed him to explore a variety of topics primarily related to the overlap that exists between various disciplines and he has been asked to develop curriculum and documentation around these areas of expertise. Dr. Swafford’s dissertation (Technology Management: Guiding Organizational Direction Now and in the Future: A Technologist’s Guide) focused on the application of technology in the overall strategic direction of an organization and how shifts in generational demographics will impact the management of technology.

Email: Richard.Swafford@orionhealth.com
Phone: (760) 533-9417
Mike Davis
ACMEcyber, LLC

Mike Davis is currently a Business Risk Management and Cyber Security Consultant / Enthusiast (Virtual CISO) and CEO of ACMEcyber, LLC. Where he provides strategic support solutions to companies / startups / organizations, as well as leading numerous security groups / initiatives

On effective security mitigations, cyber enhanced business value, privacy protection, risk / cyber insurance, etc.

Mike has over 25 years’ experience in several IT/IA/Cyber technical and operational leadership positions in many diverse government and commercial programs / venues throughout the product / service lifecycle. Mike’s principle expertise is in information assurance and cyber security, program management, systems analysis and testing, and enterprise risk management (ERM). His expertise is in the art of “complex systems and cyber security integration, with a privacy protection overview” enables him to quantify and simplify what matters most to the ERM value proposition.

In the San Diego community he serves several professional groups: ISC2 (as Pres), IEEE Cyber Security SIG (as Chair), SOoC (steering group), and actively participates in others: Infragard, ISSA, CyberTECH, INCOSE, AFCEA, etc. His qualifications are Electrical Engineer / MSEE, MA Management, with certifications in CISSP, CISO and Systems Engineering, and senior qualifications in Program Management and Risk Management. Mike is also a retired Naval Officer and federal civilian employee.

http://www.linkedin.com/in/mikedavissd

John A. Zanazzi
Janazz, LLC

John A. Zanazzi is the founder and President of Janazz, LLC. Janazz specializes in assisting small practices that are struggling or losing money because of computer, network, or technical problems. John’s team believes that achieving HIPAA compliance and integrating Hi-tech options does not have to be a huge cost for small practices.

As a Healthcare Information Technology (HIT) Consultant, John logged thousands of hours related to the HIT process, including configuring EMRs, troubleshooting networks, monitoring security, and setting up VPN’s. He also worked with several medical device companies to install, interface, and support their devices. In addition, he served as the CIO of Circle the City, a nonprofit health care clinic for the homeless.

As well as consulting, John enjoys teaching. His teaching experience had included full time CIS faculty and Health Information Technician grant director at Gateway Community College for 15 years. After retiring, John relocated to San Diego, and currently teaches for the University of Phoenix and UCSD extension.
Meet our Incredible Presenters

Rusty Sailors
LP3-SecuIT

President / CTO LP3: Responsible for the execution of five wholly owned subsidiaries and joint ventures focused on holistic security solutions. Mr. Sailors ensures the delivery of value to customers in the Intelligence Community, the Department of Defense, Special Operations community, Academia, Commercial Industry and Small and Medium sized Businesses. Chairman / CEO LP3-SecuIT: Responsible for the strategic direction and growth of an emerging commercial cyber security company focused on SMBs. Chairman Protecting Tomorrow 501(c)3: Responsible for the strategic direction and growth of a quickly growing non-profit focused on helping to secure, protect and educate students in schools, women on line, SMBs, emergency response organizations and transition veterans to successful civilian careers. Protecting Tomorrow also helps to drive security into emerging technologies from the ground up.

Academia:
Mr. Sailors is a contributing member and former Vice Chairman of the Executive Board for the UCSD Corporate Affiliates Program (CAP) and is a Fellow at the Gordon Engineering Leadership Center within the UCSD Jacobs School of Engineering. Mr. Sailors is on the founding board of CASTER, a new center at UCSD focused on driving technology leveraging the IoT and highly advanced research and technologies to assist the emergency response community. He also serves on the Cyber Technical Advisory Panel for National University, which is an accredited NSA Center of Academic Excellence in Cyber Security.

Emergency Services:
Mr. Sailors is on the Executive Board for InfraGard in San Diego; the partnership between Industry and the FBI focused on protecting critical infrastructure. Mr. Sailors is also an Infrastructure Liaison Officer (ILO) and Terrorism Liaison Officer (TLO) with the San Diego Law Enforcement Coordination Center (SDLECC).

LP3 culture fully supports community involvement and support to warfighters and veterans. As a veteran, Mr. Sailors leverages much of his military and post-military experience in serving as the Battalion Chief for Special Operations for volunteer fire and rescue response in the wildland-urban interface in the hills and mountainous areas North East of the city of San Diego. In this first responder role, Chief Sailors supports community and academic initiatives and helps to organize and manage the First Responder Advisory Panel for ARCSAFE (Architecture for Safer Schools).
Dr. Jennifer Cunningham
University of Phoenix

Dr. Jennifer Cunningham is the Assistant Dean of Competency Based Education for the University of Phoenix. Her combined experience as an educational leader, instructional designer, faculty member, entrepreneur, and student has given Jennifer a well-rounded ability to innovate and take curriculum to the next level. Her main focus over the last two years has been the strategic planning and deployment of competency education for several online institutions.

She understands the time and attention it takes to design and administer a quality competency program with superior assessments, valid competencies, and adaptive curriculum selection. Jennifer holds a Doctorate from Capella University in Education with an emphasis in Instructional Design for Online Learning, a Master’s of Leadership, and a Master’s of Information System Security.
Users: The Weakest Link in the Cybersecurity Chain

Speaker: Dr. John Sahlin, Engility

Cyber security breaches are part of the new normal in today’s ever-connected world. A recent evaluation of the top 1,000,000 Internet Domains evaluated more than one-third as “risky” from a cybersecurity perspective (Menlo Security, 2015). The U.S. Federal Bureau of Investigation reported that the 2014 breach of Sony Pictures was organized and highly sophisticated, indicating that the attack would have been successful in defeating 90% of the network defenses used in private industry and would have been able to “challenge state government” (Rosenblatt, 2014). Given these reports, is cybersecurity even possible?

The Military’s and Government’s War Against Cyber Security

Speaker: Rusty Sargent, San Diego Digital Forensics

Military leaders want private sector and National Guard cyber professionals ready in case of a national network emergency. The Pentagon is prepared to draft thousands of private sector and National Guard cyber pros in the event of a network emergency affecting American lives, a top U.S. military official reported in April of this year. During this session, guests will learn about how far the Military and Government have come, where they are today, and where they plan to be in their efforts to combat cyber-attack, and the relationship with private sectors.
The Cyber Threat Landscape
Speakers: Special Agent Jason Pearson & Supervisory Special Agent Terry Reed, Federal Bureau of Investigation (FBI), San Diego

The reality of today’s cyber threat landscape involves one’s adversary overlapping many categories of threat actors. Cybercriminals work alongside Hactivists and worse. There are well-documented “conscious collusions” between nation states and organized cyber-criminal groups. Follow the FBI through their pursuit of cyber threats throughout digital worlds. Learn how the FBI exposes hackers and works with industry leaders in safeguarding their organizations’ assets. This session will educate guests on what the cyber threat landscape comprises, build awareness of cyber-attacks, and learn preventative techniques to protect one’s assets and maintain safety.

Business Driven Technology
Speaker: Dr. Jennifer Cunningham, Assistant Dean of Competency Based Education

Have you ever wondered what drives technology? Is it business needs? Is it because technology can sparkle? Why does it seem like a great idea when proposed, but when adapted falls short of expectations? In this session, we will examine some of the business driven technologies that have been implemented over the last past 20 years, some with great success, and others that have fallen completely flat on its expectations. We will also look at new technology that will be entering the market place near you and determine if the business will be driving the technology or the technology driving the business.

Breaking into IT
Speaker: Joe Lodewyck

Learn about trending certifications that empower movement into various IT job fields, and what it takes to ‘break into IT’ for those who seek the challenge.
What Does It Mean to be HIPAA Compliant?
Speaker: John A. Zinazzi

If you ask people, “What does it mean to be HIPAA compliant?” you will hear several different answers. In the eyes of the Healthcare Industry’s Information Security Leaders, the definition goes beyond quoting the basic regulations.
In order for your practice to be HIPAA compliant, there are a number of things that must be done.
This will include:
- Ten easy things you can do increase your local workstation security
- Top 10 Myths of Security Risk Analysis
- All attendees will receive HIPAA/HITECH Security Checklist and a sample Business Associate Agreements.
This session will enlighten guests, present the Information Security’s stance on HIPAA Compliance and what is needed to guarantee compliance has been met.

Cloud and Mobile Security, Just the Facts, Key Concerns, and Mitigations
Speaker: Mike Davis

Your organization is likely ‘all in’ on expanding the use of cloud and mobile for improved performance and user experience, as well as resource efficiencies. Yet those two areas are also huge threat vectors for the cyber bad guys with the Inherent volume and leverage they gain by ONE attack and entry.
So what are the current risks and accepted mitigations to minimize the risk posture affordably? We will describe those in detail as well as provide a comprehensive position paper for each.
Cyber Maturity, Information Governance and Managing Cyber Risk: Is Your Customers’ Information Safe with You?

Speaker: Dean Larsen

Cyber security is an important concern for every organization. Daily occurrences demonstrate the risk posed by cyber attackers—from individual, opportunistic hackers, to professional and organized groups of cyber criminals with strategies for systematically stealing intellectual property and disrupting business.

The management of any organization faces the task of ensuring that its organization understands the risks and sets the right priorities. This is no easy task in light of the technical jargon involved and the pace of change.

Focusing on technology alone to address these issues is not enough. Effectively managing cyber risk means putting in place the right governance and the right supporting processes, along with the right enabling technology.

This complexity, however, cannot be an excuse for company management to divest responsibility to technical “experts.” It is essential that leaders take control of allocating resources to deal with cyber security, actively manage governance and decision making over cyber security, and build an informed and knowledgeable organizational culture.

This session will cover the world of cybercrime today, explore five common cyber security mistakes, explain the importance of customizing cyber security policies, outline the critical dimensions of a strong cyber security model, and look at key questions to help you navigate the “new normal” of cyber security.

What I have learned as CISO – 2 years and counting…

Speaker: Gary Hayslip

Have you ever wondered what the life of a CISO entails? Explore the Good, the Bad, and the Ugly of the challenges, opportunities, and rewards of being a CISO through the experience and eyes of Gary Hayslip, CISO for the City of San Diego.
White, Gray, Black – Which are you?  
Hacking Trends, Tools, and Challenges  

Speaker: Brandon Kravitz

Hackers come in all shapes and sizes, and apparently colors, too. You have your White Hackers, your Gray Hackers, and your Black Hackers. Have you ever wondered what tools these hackers use or what impact they have on our businesses, personal accounts, and our general security? This session will help you understand the hackers’ world, some of the nifty tools being used, what’s trending, and the challenges most organizations face.

Hackersponders  

Speaker: Rusty Sailors

As a Battalion Chief in the fire service, we use emerging tools to collect critical field information for first responders during large incidents - like the wild fires here in Southern California. This talk bridges from the physical security of firefighters to the cyber security of firefighters. Most people don't know our first responders are under attack (from both physical and cyber perspectives) and this talk demonstrates some of both.

Privacy, Security and Compliance: Who can see my Health Information and Why?  

Speaker: Dr. Richard Swafford

Everyone who visits a healthcare facility is asked to sign a document, which informs each person about his/her privacy and rights as a patient. Most people feel content upon signing the Privacy form and believe their health information is safely tucked away in the healthcare facilities’ vaults. Do you believe your health information is safe? Learn about healthcare security challenges and what you could do to protect yourself.
Topics / Presentations

Data Security – What exactly is that, and where does Privacy fit in?
Speaker: Mike Davis

Since most would agree that DATA is an organization’s most valuable asset, including IP, clients’ lists, proprietary processes, etc., just what are the key cyber data threats? In addition, with all the news about mega privacy breeches from major companies (SONY, Anthem, etc.) how can an organization build in data security and accommodate privacy by design?
Where it does not matter what part of the data business you are in, from “big data” to predictive analytics to internet of things (IoT) and everything in between – ” data security” must be a built in capability or your product / services can be marginalized or even used against the client. Data breaches happen to every size of an organization and the huge fines and lost reputation can kill a small company.
We will cover what really matters in data security and how to build in Privacy by Design (PbD).

Protecting Children from Online Threats

Do you know who is talking to your children on the Internet?
Do you know what websites your children visit?

Speaker: Brendan McHugh, DDA

Knowing the places and people your children "visit" online is just as important as knowing their friends and the places they go in the real world. Unless you know what your child is doing in cyberspace, he or she could be in danger. Every minute of the day, children are solicited and...
Defending the Defenders

Speaker: Craig Rosen, FireEye

The threat landscape has changed. Cybercriminals and nation-states are aggressively pursuing valuable data assets, such as financial transaction information, product design blueprints, user credentials to sensitive systems, and other intellectual property. Simply put, the cyber offense has outpaced the defensive technologies used by most companies today. The new generation of threats happens over multiple stages across several threat vectors when penetrating a network and then extracting valued information. Cybercriminals combine Web, email, and file-based attack vectors in a staged attack, making it far more likely for their attacks to go undetected. Today’s firewalls, IPS, AV, and Web gateways have little chance to stop attackers using zero-day, one-time-use malware, and APT tactics. This session will help guests gain an understanding of FireEye’s role in supporting industry leaders in an effort to minimize damage from on-going cyber-attacks, and demonstrates how FireEye defends those who are trying to defend our nation.

Cybercrime issues and what you could do about them

Speaker: Sergeant Mark Varnau, San Diego County Sheriff’s Department

Cybercrimes, once the domain of undaunted genius teenagers as portrayed in the movies “War Games” and “Hackers,” has grown into a mature and sophisticated threat to everyone connected to the Internet. Have you wondered – “What are these cybercrimes?” and “What could I do about them?” This session will discuss cybercrime issues, and include some suggestions from our experience in dealing with them.
Security Implications of Multi-tenancy: From On-premise to Cloud Services

Speaker: Matt Stamper

Understanding the implications of multi-tenancy on security is a critical topic for most organizations. Knowing how multi-tenancy impacts service delivery, roles & responsibilities, and risk is a skill that IT departments need to foster within their organizations. This discussion looks at multi-tenancy across multiple service-delivery models ranging from colocation to cloud services as well as assessing the impacts by each specific IT layer (e.g. application, database, servers, storage, networks, and backups). Coming out of the presentation, participants will know important risk considerations that should be assessed for their organization’s portfolio of applications and they will be better prepared to evaluate the security implications that are specific to their IT environment.

Grabit Malware, Moose Router Worm, Android Ransomware, Hacking Commercial Aircraft – the newest bad stuff and how to fight them…

Speaker: David O’Berry

Learn what it takes to uncover the newest bad stuff and how to fight the newest bad stuff. Guests will be taken on a journey through discovering and detecting new malware, viruses, worms – cyber-attacks, and learn how to defend against these nasty, financially damaging, and destructive apps.
CONFERENCE SCHEDULE

- 9:00am – 10:00am: Keynote Speaker
- 10:15am – 11:00am: Session I
- 11:30am – 1:00pm: Lunch ‘n’ Learn
- 1:15pm – 2:00pm: Session II
- 2:15pm – 3:00pm: Session III
- 3:15pm – 4:00pm: Session IV

8:00 am – 9:00 am

Registration

- Lobby
- Refreshments
- Room 105
- Vendor & Presenter Check-in/Lounge
- Room 104

9:00 am – 10:00 am

Keynote Speaker

- Introductions: Liane Monaco Christensen, CCC, College of IS&T
- Welcome and remarks: Dennis Bonilla, Executive Dean
- Keynote Speaker: RADM (Ret) Kenneth D. SlaghtChair, Cyber Center of Excellence

10:15 am – 11:00 am

Session I

- Room 108
- Dr. John Sahlin, Engility
- Users: The Weakest Link in the Cybersecurity Chain
- Room 109
- Rusty Sargent, San Diego Forensics
- The Military’s and Government’s War Against Cyber Security
- Room 110
- Supervising Special Agent, Terry Reed and Special Agent, Jason Pearson, Federal Bureau of Investigation (FBI), Cyber Intelligence Division
- The Cyber Threat Landscape9: Elizabeth Meade
- Room 111
- Dr. Jennifer Cunningham, Assistant Dean of Competency Based Learning, School of Business, University of Phoenix
- Business Driven Technology
- Room 112
- Joe Lodewyck, Associate Dean of Assessment, College of Information Systems and Technology, University of Phoenix
- Breaking into IT
- Room 113
- John A. Zinazzi, Janazz, LLC
- What Does It Mean to be HIPAA Compliant?
- Room 114
- Mike Davis, ACMEmber, LLC
- Cloud and Mobile Security, just the facts, key concerns, and mitigations.
- Room 115
- Dean Larsen, KPMG
- Cyber Maturity, Information Governance and Managing Cyber Risk: Is Your Customers’ Information Safe with You?
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Panelists</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:30am – 1:00pm</td>
<td>Lunch</td>
<td></td>
<td>Room 105</td>
</tr>
<tr>
<td>1:15 pm – 2:00pm</td>
<td>Lunch ‘n’ Learn Panel Discussion/Q&amp;A featuring:</td>
<td>Mandy Griffith, DOJ; Rusty Sargent, SD Digital Forensics; Brendan McHugh, SD DDA; Craig Rosen, FireEye; David O'Berry, McAfee/Intel; Shirley Adams, CyberTECH; Sabrina Feve, DOJCaptain; Lon Turner, CV PD; Sergeant Varnau, SDCSD; Matt Stamper, redIT</td>
<td>Room 106 &amp; 107</td>
</tr>
<tr>
<td>1:15 pm – 2:00pm</td>
<td>Meet 'n' Greet: Post Panel Discussion Q/A</td>
<td></td>
<td>Room 106 &amp; 107</td>
</tr>
<tr>
<td>1:15 pm – 2:00 pm</td>
<td>Session II</td>
<td>Dr. John Sahlin, Engility; Gary Hayslip, City of San Diego; Brandon Kravitz, Senior Software Developer and Technology Enthusiast, Jungo; Rusty Sailors, LP3-SecurIT; Joe Lodewyck, Associate Dean of Assessment, College of Information Systems and Technology; Richard Swafford, Orion Health Inc., UOPX Faculty; Mike Davis, ACMEcyber, LLC; Dean Larsen, KPMG</td>
<td>Room 108 Room 109 Room 110 Room 111 Room 112 Room 113 Room 114 Room 115</td>
</tr>
</tbody>
</table>

To learn more about what our Cyber Security Industry Experts are doing, stick around and continue getting to know the details behind the Firewall.
### Session III

2:15 pm – 3:00 pm

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker/Title</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:15 pm</td>
<td>Session III</td>
<td>Brendan McHugh, DDA, San Diego District Attorney's Office</td>
<td>Room 108</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Protecting Children from Online Threats</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Gary Hayslip, City of San Diego</td>
<td>Room 109</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>What I have learned as CISO - 2 years and counting...</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Craig Rosen, Vice President and Chief Security Officer, FireEye</td>
<td>Room 110</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Defending the Defenders</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Dr. Jennifer Cunningham, Assistant Dean of Competency Based Learning, University of Phoenix</td>
<td>Room 111</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>School of Business, University of Phoenix</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Business Driven Technology</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Sergeant Mark Varnau, San Diego County Sheriff's Department</td>
<td>Room 112</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Cybercrime issues and what you could do about them</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>John A. Zinazzi, Janazz, LLC</td>
<td>Room 113</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>What Does It Mean to be HIPAA Compliant?</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>David O'Berry, MacAfee</td>
<td>Room 114</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Grabit Malware, Moose Router Worm, Android Ransomware, Hacking</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Commercial Aircraft – the newest bad stuff and how to fight them...</td>
<td></td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Matt Stamper, redIT</td>
<td>Room 115</td>
</tr>
<tr>
<td>2:15 pm</td>
<td></td>
<td>Security Implications of Multi-tenancy: From On-premise to Cloud Service</td>
<td></td>
</tr>
</tbody>
</table>

### Session IV

3:15 pm – 4:00 pm

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker/Title</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:15 pm</td>
<td>Session IV</td>
<td>Brendan McHugh, DDA, San Diego District Attorney's Office</td>
<td>Room 108</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Protecting Children from Online Threats</td>
<td></td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Brandon Kravitz, Senior Software Developer and Technology Enthusiast, Jungo</td>
<td>Room 109</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>White, Gray, Black - Which are you? Hacking Trends, Tools, and Challenges.</td>
<td></td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Craig Rosen, Vice President and Chief Security Officer, FireEye</td>
<td>Room 110</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Defending the Defenders</td>
<td></td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Rusty Sailors, LP3-SecurIT</td>
<td>Room 111</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Hackersponders</td>
<td></td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Sergeant Mark Varnau, San Diego County Sheriff's Department</td>
<td>Room 112</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Cybercrime issues and what you could do about them</td>
<td></td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Richard Swafford, Orion Health Inc., UOPX Faculty</td>
<td>Room 113</td>
</tr>
<tr>
<td>3:15 pm</td>
<td></td>
<td>Privacy, Security and Compliance: Who can see my Health Information and Why?</td>
<td></td>
</tr>
</tbody>
</table>
David O'Berry, MacAfee
Grabit Malware, Moose Router Worm, Android Ransomware, Hacking Commercial Aircraft – the newest bad stuff and how to fight them...

Matt Stamper, redIT
Security Implications of Multi-tenancy: From On-premise to Cloud Service

Room 114
Room 115
Thank you for attending!

University of Phoenix
CyberCon 2015

Special thanks to those who contributed to the success of this event, including and not limited to...

Nan Mac Isaac, JD, Director of Academic Affairs
Carly Ward, Project Manager
Dennis Bonilla, Executive Dean, College of IS&T
Dr. Brad Purdy, Program Dean of Emerging Technology, College of IS&T
Paul Porch, Dean of Faculty, College of IS&T
Liane Monaco-Christensen, Campus College Chair, College of IS&T
Dr. Tony Lopez, Lead Faculty Area Chair, College of IS&T
Brenda Holland, Associate Faculty, College of IS&T
Castle Phelps, Associate Faculty, College of IS&T
Sanford Schram, Associate Faculty, College of IS&T
Richard Swafford, Associate Faculty, College of IS&T
Michael Taousakis, Associate Faculty, College of IS&T
Maggey Felix, Director, Marketing & Operations for CyberUnited
Jenny Woudenberg, Marketing and Operations Manager, CyberUnited
Lynda Majerowicz, Alumni
Richard DeSio, Alumni
Susan Fredricks, Alumni
Cheryl Faye, Student
Joseph A. DeSio, Jr, Consultant
Dominic Monaco, Volunteer
Stacey McRae, Volunteer
College of Information Systems & Technology

IT powers today’s world and we can help you power IT. With the right set of skills, you can tackle the demands of this fast-paced industry. Our degree and certificate programs provide the industry-relevant knowledge and tools that can open doors in your career. The College of Information Systems and Technology offers:

Industry-aligned certificates: Our certificate programs can help prepare you for one or more of over 40 key industry certifications, from companies like Microsoft®, Cisco®, and Oracle®, and, with no additional tuition or time, you can earn a certificate program as you work toward your degree.

Industry tools: Our interactive curriculum gives you virtual access to tools used by IT professionals and to training materials that further prepare you for industry certification.

Contact Us

University of Phoenix, San Diego Campus
9645 Granite Ridge Dr.
San Diego, CA 92123

Email: Liane.Monaco@phoenix.edu