Interconnecting the Building Blocks of a Secure Cyber Ecosystem

ISACA®
Trust in, and value from, information systems
Silicon Valley Chapter

ISACA-Silicon Valley

2015 Spring Conference

May 14-15, 2015 at the Biltmore Hotel in Santa Clara, California

Contents

Welcome

Six months ago, ISACA-SV's Fall 2014 Conference endeavored to explore what has historically made Silicon Valley such a hotbed of innovation and how the area's unique environment has been reflected in our fields of information security and audit. Recognition of the importance of Silicon Valley to evolving technology, acceptance and shaping of technology use, and security and privacy was further underscored with an event three months ago. The White House Summit on Cybersecurity and Consumer Protection was held 13 February 2015 at Stanford University. President Barack Obama used the event to sign an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. The Summit announced the Obama Administration's priorities to strengthen the country's approach to cybersecurity threats by:

1) **Protecting the country's critical infrastructure – our most important information systems – from cyber threats.**
2) **Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.**
3) **Engaging with international partners to promote Internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.**
4) **Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.**
5) **Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.**

According to Gartner, worldwide spending on information security approached $71.1 billion in 2014. Just in 2014 alone, more than 100 million U.S. businesses and individuals were affected by online-related fraud or theft. Company names such as Target, Home Depot, eBay, Anthem, and Neiman Marcus, and federal agencies such as the U.S. Postal Service, the U.S. Nuclear Regulatory Commission, and the White House were splashed on the front page as cyberattack victims, or worse, in a case of 'dog bites man' tedium, were buried on an inside page. Besides the reputation-damaging repercussions, with the cost of a breach currently averaging between $3 million and $5 million, all corporate Boards should be concerned.

Cybersecurity is finally being recognized as a national security and public safety issue. Cyber-security-related terrorist threats to governments and companies have increased fivefold since 2009, most notably the Sony Pictures Entertainment hack alleged by U.S. intelligence officials to have been conducted by agents of the North Korean government.

The Administration's above five priorities are to be supported by increased Public-Private collaboration on cybersecurity and institutionalized sharing of cybersecurity information. Rapid and substantive information sharing is essential to enable U.S. companies to work together to identify threat trending and to respond to actualized threats, rather than inefficiently working alone with incomplete information and perspective. However, what are the implications of this information sharing to privacy and civil liberties, and are associated protections adequate to protect individuals and competing companies?

The Summit's call for increased Government-Private Sector cooperation may strike tension in freewheeling Silicon Valley, but it actually underscores area companies' historical collaborating with Government. Probably a majority of Silicon Valley's best inventions can be traced back to having received the support of DoD

and government agency funding (GPS, IOS's Siri, Google's search algorithm, self-driving cars, IDS technology, and most famously the Internet itself). How successful will these efforts to collaborate on cybersecurity be?

An evolving trend is that cyberattacks are increasingly becoming attempts to steal data for monetized benefit. Not to say that business disruption and theft of intellectual property don't still remain as exploit goals. But now companies whose businesses involve storing data are becoming targets that were before seen as unlikely to be very appealing, such as health care networks and government agencies. What new technologies, processes, and audit approaches can be adopted to help protect these new targets?

Over the next two days we will be calling to the podium a number of local security and audit professionals. They will be educating us with lessons learned and thoughts of what the future holds. We have 16 CPEs worth of insight and provocative ideas to look forward to, buttressed by networking and the professional camaraderie that has become the hallmark of ISACA-Silicon Valley Chapter. We hope that you enjoy!

Conference Committee

The Chapter could not provide this wonderful opportunity to learn, network and earn CPEs without the efforts of the Conference Committee. Many thanks go out to each member of the Conference Committee.

- **Ruchi Gupta**, Conference Director
- **Larry Halme**, Vice President
- **Teresa Huang**, Speaker Liaison
- **Mike Jordan**, President
- **Shun Ye**, Sponsor Liaison

Our Volunteers

Another group that makes these conferences possible are the dedicated volunteers. These individuals, many of whom are members of the San Jose State University ISACA Student Group, keep all the workings of the conference well-oiled while catering to attendee's needs. Many thanks to:

Mustafa Alseddiq	Greg Edwards	Laisz Lam
Ryan Anderson	Sheemul Gupta	EJ Romero
Ana Casalco	Nitya Kashyap	Anna Song
Lucas Chung	Harman Kaur	

Program Schedule: Day 1 (May 14th 2015)

Time		Session	Speaker
8:00 AM		**Registration, Networking & Breakfast**	
8:45 AM		**Welcome Message from the ISACA – SV Board**	
9:00 AM	**1-1**	**Session 1 – Opening Keynote: Security Transformation** The need for a Security Transformation in the enterprise has been clear to our industry for quite some time and the struggle to protect our data in today's business environment has been a main focus. At the same time, in an increasingly mobile-centric workforce, organizations are dealing with the shift from analog to digital and require more compliance and policy to protect against breaches, lack of transparency and accountability. To keep up with these changing demands, IT decision makers and their organizations must be more agile, manageable and responsive to a different set of challenges that arise. Join this session to hear Justin Somaini, Chief Trust Officer at Box, detail what security transformation will look like in the coming year and how it will redefine the responsibilities of vendors, cloud providers, and security practitioners to resolve one of the most significant security problems of the past 40 years.	**Justin Somaini** Chief Trust Officer, BOX
9:55 AM	**1-2**	**Session 2 – Security for Today, Prepared for Tomorrow** We all know that the world is changing and the latest cliché is "breaches are the new norm." Is this really the case and are we willing to accept this as a fact? Maybe or maybe not, but one thing is clear, things are always changing and security is no exception because it has to keep up with the trends and technologies of today. Security also has to anticipate new trends and the future to be scalable and flexible enough to adopt and apply to the unknown. There are steps the security industry and professionals can take to help focus on today and future. Some are tried and true best practices and others involve a re-imagination of security.	**Adam Shnider** CISO, Riverbed Technologies
10:45AM		**Break**	
11:00 AM	**1-3**	**Session 3 - Balancing Speed and Security to Power Growth at Enterprise Startups** Think speed and security don't go together? Think again. In the world of enterprise startups, agility and speed of delivery is key to attracting business from large enterprise clients. When your clients expect consistently high quality security and risk management, how can you keep up with the startup rate of growth? In this talk, we will discuss the nuts and bolts of a creative security team that is geared towards securely enabling supercharged growth of the company (think 80%+ YoY). We will discuss the foundational security structure needed to support various groups within the company, and also the strategic approach to positioning security within the organization so it becomes an integral part of the DNA. We will talk about what has worked for Medallia and what we have learned by experience working with some of the largest and most conservative organizations in the world.	**Harshil Parikh** Head of Security and Compliance, Medallia, Inc.
11:55 AM	**1-4a**	**Platinum Sponsor Session 1 - BPM**	

Time		Session	Speaker
12:25 PM		**Lunch**	
1:10 PM	**1-4b**	**Platinum Sponsor Session 2 - SOAProjects**	
1:40 PM	**1-5**	**Session 5 - Securely scaling an enterprise business cloud: prerequisites, process, and proof** Increasingly, the security -- and the privacy -- of sensitive corporate IP, corporate identity, and customer PII is placed in the hands of cloud vendors. Increasingly, this is done without sufficiently establishing the true risks that a given vendor presents. In this session, we present a proven, efficient, scalable approach to cloud vendor assessment, analysis, and testing that can be used to protect and enable the enterprise. Takeaway for audience: Prerequisites for a secure, scalable, robust business cloud Necessity of an end-to-end process for onboarding vendors Techniques to efficiently evaluate, approve (or reject) vendors	**Doug Meier** CISO, Pandora
2:35 PM	**1-6**	**Session 6 - Security Concerns in Financial Services – Opportunities or Threats** The financial services sector comprises of the full complement from large regulated lenders, niche lenders who focus on the mid-market and small /micro ticket online lenders with a hyper focus on a specific market with each type of lender having different security concerns. Security concerns are traditionally classified into • Data privacy • Data and systems security • Business continuity and contingency planning • Liability and risk management In this session, I would like to explore if security concerns will inhibit growth or provide new opportunities in Financial Services by discussing: • New terms being coined like Extraterritoriality • What are their potential market disrupters? • How are different constituents reacting to security concerns?	**Mukul Mittal** Executive Vice-President, Cloud Lending Inc.
3:25 PM		**Break**	
3:40 PM	**1-7**	**Session 7 - Managing Security Risks Affecting Robots, Implantable Devices, and Other Disruptive Technologies."** What are the new information security legal challenges in an era of rapid, sweeping changes in technology? Enterprises face compliance and liability issues from the use of robots, artificial intelligence systems, non-traditional mobile devices, Big Data, the Internet of Things, augmented and virtual reality systems, 3D printing, wearables, and implantables. This talk will cover the intersection among legal, business, and technology issues from the deployment of these disruptive technologies and ways enterprises can manage their legal risks.	**Stephen S. Wu** Silicon Valley Law Group

Time		Session	Speaker
4:35 PM	**1-8**	**Session 8 – Panel Discussion on Cyber Insurance** Cyber insurance is a product designed to protect businesses from information technology, infrastructure, and Internet-based risks such as cyber-attacks, theft or loss of information, and disruption of services. The panel will help provide guidance to determine the appropriate level of cyber insurance coverage required by businesses. The panel will also look at what's typically covered by cyber insurance, under what conditions, and include some case studies to help illustrate key points. New research from CyberEdge Group reports 52% of security professionals who were surveyed believe their organizations will likely be successfully hacked in the next 12 months. And according to the 2014 Cost of Data Breach Study commissioned by IBM, the average cost of a security breach was $3.5M, a 15% increase from the previous year. Cyber insurance is quickly becoming a risk mitigation tool for businesses that use information technology to process/store sensitive data and information. Discussion topics will range from forensics and investigations, litigation, settlement and damages, breach notifications, business continuity, proper levels of coverage, and factors that determine the cost of premiums.	**Brian Bertacini (Moderator)** President & CEO, AppSec Consulting, Inc. **Daniel Bozutto** Broker, Bozutto & Associates Insurance Services **Julie Lewis** President & CEO, Digital Mountain **Stephen S. Wu** Silicon Valley Law Group
5:30 PM		**Reception and Networking** Please join the Conference Committee and Board of Directors for hors d'oeuvres, fine wine, beer and sodas in a relaxing social setting meant to encourage networking.	
7:00 PM		**Day 1 ends**	

Program Schedule: Day 2 (May 15th 2015)

Time		Session	Speaker
8:00 am		**Registration, Networking & Breakfast**	
8:45 AM		**Welcome Message from the ISACA – SV Board**	
9:00 AM	**2-1**	**Session 1 – NIST Cyber Security Framework and how it is Impacting Government and Enterprises** NIST Cyber Security Framework, providing a short overview of it and then exploring its relationship with other standards/frameworks, how it's being used, its impact, etc.	**Eric Hibbard** CTO, Security and Privacy Hitachi Data Systems
9:55 AM	**2-2**	**Session 2 – Toward Cyber Security in Business Terms: Quantifying the Risk in Dollars Experience** Corporate executives know that while cyber risk cannot be eliminated, it can and must be managed so as to minimize impact on the business. But it is difficult to manage a risk that cannot be measured. Unless companies can identify and quantify cyber risks in dollars, they cannot effectively allocate security resources, justify investments, weigh competing priorities, or communicate risk with internal stakeholders or concerned customers. In January the World Economic Forum and Deloitte proposed a framework for a quantitative, risk-based approach to cyber security focusing on asset value at risk. Earlier frameworks, notably the FAIR taxonomy, have also tried to put risk assessment on a quantitative footing. Like all assessment frameworks, these approaches are based on an exhaustive set of subjective human judgments, and as a result they are laborious and of limited accuracy. We propose an automated approach using actuarial science and empirical data to quantify risk. Data on rates of occurrence and financial impact of cyber incidents are extracted from industry reports, census data, SEC filings, and other sources, aggregated using Bayesian statistics and combined with automatically measured local IT factors to build a risk profile for an organization. Value at risk can be calculated for both structured and unstructured data assets; for the latter, a statistical approach is used based on department ownership and document access patterns. Risk can be managed and mitigated strategically when quantified in dollars. Progress can be measured, and hypothetical actions can be modeled and evaluated in terms of risk. Even potential black swan events can be anticipated and managed. With quantitative risk projections companies can plan ahead to minimize impact of the most extreme cyber events.	**Thomas Lee, PhD** CEO, Vivo Security
10:45 AM		**Break**	

Time		Session	Speaker
11:00 AM	**2-3**	**Session 3 - Twenty Steps Towards A Strong Cyber Security Program** In 2008 the Secretary of Defense requested the assistance of the NSA to develop a prioritized list of security controls. This began the process that led to what is now known as the Twenty Critical Security Controls. Many organizations are now implementing the controls with great success. The US State Department reports that it was able to achieve an 88% reduction in vulnerability-based risk by implementing the controls. In this presentation John will discuss the history of the Twenty Critical Security Controls, the philosophy and approach they are based on, the components of a control, and the objective of each control. Additionally, John will discuss the process of implementing each control. Finally, John will show how organizations are implementing the controls and the real world results the Twenty Critical Controls are generating.	**John Millican** Principal The Office of CIO
11:55 PM	**2-4a**	**Session 4a – Cybersecurity and Compliance: Presenting to the Board and Non IT-Executives** We all understand cyber security as a media term that has many components and requires investment in different areas. To a board member or the CFO, who controls the purse, it is all a vague topic and a big sinking hole. Similarly IT leaders in companies with various compliance activities have to face the same music trying to explain where compliance falls short of Cyber Security. Using SOAProjects proprietary format, this presentation provides a platform to allow IT security leaders to communicate effectively to executive management.	**Jay Swaminathan** Sr. Director SOAProjects
12:25 PM		**Lunch**	
1:10 PM	**2-4b**	**Session 4b - Implementing, Maturing and Sustaining Multiple Compliance Requirements….SOC 2, ISO 27001 and FedRAMP**	**Sumit Kalra** Partner, Information Technology Audit and Compliance Services BPM

1:40 PM	**2-5**	**Session 5 – Does Audit Make us Secure?** Audits don't make us secure. It's the information we share and the programs that help management prioritize response that lead management to making us more secure. This session will speak about programs that align to the NIST Cyber Security Framework and various types of risk assessment that would inform if a cyber-security program were inadequate for business needs. Presenter will review types risk assessments, what layer of the organization evaluates what types of risk, and further explain types of follow on audits companies should perform based on what they found. Audit Risk is the risk that a test of a control would not identify or prevent the bad event from occurring. I think the presentation should instruct people about what they do with findings and how to work with management so the right people can take action on security risk.	**Robin Basham** Director Enterprise Compliance, Ellie Mae
2:35 PM	**2-6**	**Session 6 - Leveraging Pen Testing to Augment an Audit** Auditing and Pen Testing are both disciplines that find system weaknesses and confirm strengths for a customer who doesn't necessarily embrace the activity and resists accepting the results. In this talk I will discuss the phases of a Pen Test, and how that emulates a real cyber or physical attack, how Pen Tester's activities differ from real attacks, and the methods used to prove results while doing no harm. I will discuss how an audit can leverage Pen Testing to provide a customer a better overall assessment of their environment and the challenges of creating a final report that the customer can understand and is actionable. After completing this session, participants will be able to: 1. Understand the five phases of a Pen Test 2. Differentiate between a Pen Test and an Attack 3. Benefit from the knowledge of how Pen Testing can augment Audit activities **4.** Utilize the gained insights into the similar challenges Auditors and Pen Testers face	**Lee Neely** Sr. IT and Security Professional Lawrence Livermore National Laboratory
3:25 PM		**Break**	

3:40PM	**2-7**	**Session 7 - Securing the Human Factor** Human error accounts for 52 percent of the root cause of security breaches, according to a new study from CompTIA. Asked about the top examples of human error, 42 percent of those surveyed cited "end user failure to follow policies and procedures," another 42 percent cited "general carelessness," 31 percent named "failure to get up to speed on new threats," 29 percent named "lack of expertise with websites/applications," and 26 percent cited "IT staff failure to follow policies and procedures". Companies generally rate human error as a lower concern among other security issues and this is largely due to uncertainty around how to attack the problem. The session covers several complementary approaches to attacking the problems - new employee orientation, ongoing security training program, random security audits, policy enforcement, sanctions, social engineering tests and integrating this into your environment to develop a holistic solution. The speakers individually have 10+ years of experience managing risks including the human factor for Fortune 500 companies and technology startups. The session will be interactive, demonstrate open source solutions and engage the audience with free tools that can be adopted today to encourage security best practices.	**Kartik Trivedi** Partner, Symosis Security **Jeff Brock** Co-Founder, Bay Mountain Security
4:35 PM	**2-8**	**Session 8 – Ending Keynote: Fool Me Once, Shame on You – Shifting Security Education from a Negative to Positive** The last 5 years have seen an upsurge in security education that in an attempt to innovate include simulations of attacks. This has had an adverse effect of breeding negativity in workplaces where security is often already seen as the "No Patrol". Deacon and Manke will present how to incorporate real world examples and simulations that don't leave employees feeling tricked or the victims of deceit across industries and with particular examples for the varied demographics within organizations.	**Rick Deacon** Founder of Apozy **Samantha Manke** Director at Apozy
5:20 PM		**Conference Adjourned**	

Our Speakers (ordered alphabetically by last name)

Robin Basham, Director Enterprise Compliance, Ellie Mae

Robin has served in governance and risk management roles for more than 30 years, and is most known for implementation and design of GRC Systems. Robin is responsible for the platforms, methods and execution of an overall GRC Strategy at Ellie Mae. Accomplishments include meeting the FFIEC, SOX, SOC and IS27K standards for controls and compliance. Prior to joining Ellie Mae, Robin founded Enterprise GRC Solutions, used by numerous Silicon Valley and East Bay clients to implement CobiT, ISO, NIST and ITIL compliant products and programs resulting in improved controls and greater capacity for business growth. Robin served on the ISACA SV Board of Directors, leading and participating in many East Bay conferences. Her past positions have also included Sr. Director, Enterprise GRC for SOAProjects, and Director, IT Regulatory Compliance for Control Solutions International. Before moving to California, Robin lived in New England, with employment at State Street Bank, One Communications, and International Network Services. She is known as a GRC, Cloud Security, and Sustainable Enterprise thought leader providing strategic direction to public and private corporate enterprise security and technology, and a compliance business driver with more than 100 clients served. Noted as a Master Educator, Enterprise ICT GRC Architect, Archer Certified Practitioner, and early adopter in both certifying and offering certification programs for Cloud and Virtualization, her companies extend Project Management, Training, Audit, Risk and Compliance. Maintaining a 30 year record, Robin's efforts result in on time product delivery, Sarbanes-Oxley, HIPAA, ISO 9001 and ISO/IEC 27002 , ISO 20000, PCI DSS, and SSAE no 16 unqualified Big Four adoption and opinion. Efforts across industries such as SAAS, Healthcare, Banking, High Tech, resulted in implemented sustainable processes, programs, safeguards and controls. Robin has two masters degrees, in Education and Information Technology, is a CISA, CRISC, CGEIT, HISP, CRP and VRP.

Brian Bertacini, President & CEO, AppSec Consulting, Inc.

Brian Bertacini founded AppSec Consulting in 2005, since then the company has become a leading provider of IT security testing service, information security program development, compliance validation, training and security technology integration for businesses of all sizes including starts-up and large global enterprise clients. Mr. Bertacini is a member of ISSA, ISACA, and OWASP. He has more than 20 years' experience in software development, systems engineering and information security, fulfilling various roles at IBM, Varian and Fujitsu. Brian is the founding member of the Silicon Valley OWASP chapter and he oversees the management of AppSec Consulting to ensure the company's valued clients receive the highest quality of service.

Daniel Bozzuto, Broker, Bozutto & Associates Insurance Services

I am a San Jose native and am happy to do my part in keeping the Valley great. Since I joined Bozzuto & Associates my focus has been set on Errors & Omissions, Employment Practice Liability, Directors & Officers Liability, and Cyber Liability. These coverages have been crucial for the tech industry and are continuing to grow in importance outside of it. My goal with my clients is to successfully integrate my team with theirs, set up the proper risk management procedures, and give them one less thing to worry about in their business.

Jeff Brock, Co-Founder, Bay Mountain Security, LLC.

Jeff Brock is Co-Founder of Bay Mountain Security, LLC. They focus on providing the ultimate in Cyber security management, strategy, governance, architecture, frameworks, and program execution. Bay Mountain Security compliance services include designing controls for state of the art cloud operations, compliance auditing, as well as implementations for regulatory accreditation and certifications. Jeff is a Sumo Logic customer advisory board member, and previously sat on the Akamai, Amazon Web Services, and iSEC Partners customer advisory boards, as well as on the Autodesk Executive Cloud Council.

Jeff has worked with numerous public and private companies providing valuable thought leadership and contributions to the discussion of the design, efficiency, and effectiveness of internal controls related to: AT101/SOC2 and SSAE16-SOC1 reporting, ISO27001/2 implementation and certification, Safe Harbor certification, FedRAMP/FISMA, AICPA Trust Principles, Web Trust, Sys Trust, and CSA compliance.

Jeff previously managed mission critical teams and technologies for Autodesk's Cloud Platforms division. He led highly skilled strategic teams to deliver visionary operational architecture and designs for environments, services, and products on the Auotdesk360 platform. During his 8 years with Autodesk, Jeff was instrumental in leading the charge to obtain their ISO27001 certification and operating highly available, resilient systems and products while incorporating and managing the Cloud environments globally.

Jeff is an entrepreneur and wine connoisseur. He is a vintner and General Partner of Blue Bay Wines, LLC. Blue Cellars produces internationally acclaimed wines. Prior to Bay Mountain Security and Autodesk, he helped take the Silicon Valley software company Eloquent, Inc. from startup to IPO, then through acquisition by OpenText, Inc. He also developed and implemented a medical billing and payroll system for At Home Health Care.

Rick Deacon, Founder of Apozy

Rick Deacon is an information security professional with years of experience as an ethical hacker, teacher and evangelist. Deacon is the founder of Apozy, an enterprise information security startup. Prior to starting Apozy, he could be found hacking (most notably Myspace), educating and working with Fortune 500 companies as a professional penetration tester on a daily basis.

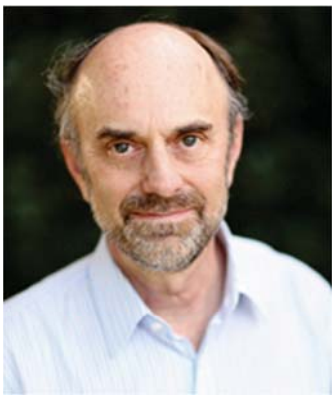
Eric Hibbard, CTO Security and Privacy, Hitachi Data Systems

Eric Hibbard is the CTO Security and Privacy in Hitachi Data Systems where he is responsible for product security strategies and oversees the integration of security and privacy measures in products and services. Mr. Hibbard is a senior security and IS auditor professional with 30+ years of experience in enterprise-class ICT, working for government (DoD, DoE, and NASA), academia (University of CA), and industry. In addition to his security and privacy duties, Mr. Hibbard serves as the Chair of the HDS Standards Council and Vice Chair of the Hitachi IT Platform Group's (ITPG) Architecture Review Board. Hibbard is actively involved in a wide range of technologies and represents Hitachi and HDS in several standards development organizations (ISO/IEC, ITU-T, INCITS) and industry associations (SNIA, TCG, DMTF, ODCA, IIC, ISACA, ISSA). He currently serves as the International Representative for INCITS/CS1 Cyber Security, Chair of the IEEE Information Assurance Standards Committee, Co-Chair of the Cloud Security Alliance International Standardization Council, Co-Chair of the ABA Electronic Discover & Digital Evidence (EDDE) Committee, Vice Chair of the ABA Cloud Computing Committee, Chair of the SNIA Security TWG, and Vice Chair of the IEEE Security in Storage WG (SISWG). In addition, he is currently the Editor of ISO/IEC 27050 (Electronic discovery), ISO/IEC 20648 (TLS for Storage Systems) and IEEE 1619 (XTS-AES) draft standards as well as the recently published ISO/IEC 27040:2015 (Storage security) and Rec. ITU-T Y.3500 | ISO/IEC 17788:2014 (Cloud computing - Overview and vocabulary). Mr. Hibbard currently holds the (ISC)2 CISSP certification with the ISSAP, ISSMP, and ISSEP concentrations as well as the ISACA CISA certification. His educational background includes a B.S. in Computer Science and a Certificate of Proficiency in Data Communications.

Sumit Kalra, Partner, Information Technology Audit and Compliance Services, BPM

Sumit Kalra has over 16 years of information technology audit, compliance and internal controls experience. His practice spans across various security standards and frameworks, including SSAE 16, ISO 27001, SOX 404, FedRAMP, regulatory compliance, and PCI. He has led security and technology audit efforts at two international accounting firms and for several companies in the technology, retail and financial industries. He has served clients in an array of industries and in various stages/situations, from startups, Cloud, SaaS to Fortune 100 companies. Currently, Sumit develops security audit methodologies at BPM, for evaluating security/compliance risks and exposures to complex on premise and cloud implementations.

Thomas Lee, PhD, CEO, Vivo Security



Thomas is a serial entrepreneur, co-founder and CEO of VivoSecurity Inc. His interest in risk quantification stems from his experience in IT and software development combined with a background in applying novel computational techniques to biological problems. He has a PhD and MS in biophysics from the University of Chicago, a BS in physics and a BS EE from the University of Washington.

Julie Lewis, President & CEO, Digital Mountain

Julie has over 20 years of experience working in the high technology industry and has managed hundreds of computer forensics and electronic discovery cases to date. Prior to founding Digital Mountain, Julie worked at VERITAS Software (now Symantec) with next-generation storage, security and Internet infrastructure companies. At VERITAS, she managed operations for new product releases across sales, marketing, product management, legal, engineering and customer support. Before joining VERITAS, Julie worked for E*TRADE. She also worked for two of the Big 4 accounting firms doing financial and IT auditing, as well as M&A due diligence as a CPA. She also worked for Applied Magnetics, a publicly traded provider of disk and tape drive components, as well as spent six years in the retail sector. Julie earned an MBA under fellowship from the F.W. Olin Graduate School of Business at Babson College and a BA in both Business Economics and Sociology from the University of California at Santa Barbara. She is a member of the High Tech Crime Investigation Association (HTCIA), National Association of Litigation Support Managers (NALSM), Sedona Conference's Working Group on E-mail Management and Archiving, and has received her EnCE (Encase Certification in Computer Forensics). Julie is founding Co-Chair of the Silicon Valley Chapter of Women in eDiscovery.

Samantha Manke, Director of Product, Apozy

Samantha Manke is the Director of Product at Apozy, where she leads the development of enterprise security gamified learning. Previously, Manke co-designed and implemented highly acclaimed security awareness programs for the Fortune 500. She presents at conferences around the world. Additionally, she has been featured in major security industry publications including SC Magazine, Computerworld and CSO Online.

Doug Meier, CISO, Pandora

Doug has 20+ years of experience designing, staffing, and managing Enterprise Architecture, Enterprise Security, Information Security, IT GRC, and related programs for Silicon Valley Internet companies. He likes the daily challenge of directing teams of talented people on critical business initiatives. He likes the excitement of bringing talented people together to solve business problems. And he enjoys working independently on program planning, security research and investigation, and vendor technology assessment and evaluation. Doug defines teamwork as taking ownership of problems and solutions, taking responsibility for communicating, and following through until the job is done. That's the main reason he has been successful in a range of corporate cultures in Silicon Valley, from start-up to global enterprise.

John Millican, Principal, The Office of CIO

John is currently a Principal with the Office of the CIO providing executive level information security services to Bay Area organizations. He has forty-six years of experience in iT including stints as CISO for Expedia Inc., and VP of IT Operations at Hotwire. John was the first person certified by the SANS Institute in the assessment and implementation of the Twenty Critical Security Controls.

Mukul Mittal, Executive Vice-President, Cloud Lending Inc.

Mukul leads product development at Cloud Lending and is closely involved in product design, development and delivery. Mukul has over 20 years of experience in software product development, project management and systems implementation, and has deep understanding of financial services industry, especially equipment leasing. Mukul has held senior positions for companies like Oracle, ITC Classic Finance and Bell Controls, where he successfully assisted clients across the world define the strategic and tactical roadmap, and effectively implement solutions under tight timelines. With his vast experience, Mukul is passionate about financial services applications that enable clients to simplify their processes and improve customer experience. Mukul graduated from Osmania University, and is a member of Institute of Chartered Accountants of India.

Lee Neely, Sr. IT and Security Professional, Lawrence Livermore National Security

Lee Neely is a senior IT and security professional at Lawrence Livermore National Laboratory (LLNL) with over 25 years of experience. He has been involved in many aspects of IT from system integration and quality testing to system and security architecture since 1986. He has had extensive experience with a wide variety of technology and applications from point implementations to enterprise solutions. Lee has worked with securing information systems since he installed his first firewall in 1989. As part of his employers Cyber Security Program (CSP) he leads their new technology group, working with programs to develop secure implementations of new technology. Lee was instrumental in developing their secure configurations, risk assessments and policy updates required for iOS, Android, BlackBerry and Windows Mobile Devices. He has worked to evolve solutions for both corporate and BYOD requirements. Lee worked with the SANS SCORE project to develop the iOS Step-by-Step configuration guide as well as the Mobile Device Configuration Checklist which is included in the SEC 575 course. He teaches cyber security courses, including the new manager cyber security training, and Information System Security Officer training. Lee has a Bachelors in Computer Science from Cal State Hayward and holds several security certifications including GMOB, CISSP, CISA, CISM and CRISC. He is also the Technology Director for the ISC^2 East Bay Chapter.

Harshil Parikh, Head of Security and Compliance, Medallia Inc.

Harshil Parikh is currently Head of Security and Compliance at Medallia, Inc. Harshil has 10+ years of experience in technical and strategic aspects of information security, and a passion for pragmatic security risk management.
With experience in building, implementing and running information security programs at global organizations, Harshil has spent significant amount of time establishing mature security strategy, building information security capability relevant to the business, and driving implementation of controls for effective risk management.

Adam Shnider, Chief Information Security Officer, Riverbed Technologies

Mr. Shnider has extensive experience in information security, enterprise risk management and audit planning. His experience includes responsibility for information as the Chief Information Security Officer of Riverbed Technologies as well as over 15 years serving clients in financial services, retail, healthcare and other industries. He has also assisted clients in designing and implementing information security programs and architectures for a variety of industries, applications and platforms. Mr. Shnider holds numerous industry certifications including Certified Information Systems Security Professional (CISSP), Certified Information Systems, Auditor (CISA) and Certified Information Security Manager (CISM) and is a Payment Card Industry Qualified Security Assessor (QSA). He holds a Bachelor of Science degree from The Ohio State University.

Justin Somaini, VP & Chief Trust Officer, Box

Justin Somaini is VP and Chief Trust Officer at Box, where he is responsible for working globally and collaboratively across Box's growing customer base, technical operations, business development teams, and partners to ensure the company is consistently delivering on its information security commitments, investing to meet the rapidly evolving security environment, and building transparent, deeply trusted relationships with its customers.
Previously, Justin created and held the role of Chief Information Security Officer (CISO) at Yahoo!, driving security planning and operations for the company. Prior to Yahoo!, Justin was CISO of Symantec where he developed the company's Information Security Enterprise Risk Management process, worked cross-functionally to manage critical incidents to resolution and drove implementation of controls for both a significant threat environment and regulatory needs.

Jay Swaminathan, Senior Director, SOAProjects

Jay Swaminathan is a Senior Director at SOAProjects. Jay has more than 15 years of risk management, compliance and process re-engineering experience. At SOAProjects, he leads a team of risk, compliance and advisory professionals to enhance their client's business process and efficiencies. Jay and his team bring a blend of practical and innovative solutions to the workplace to solve various challenges. Before SOAProjects, Jay had worked at various companies like EY and Oracle. He served as President of ISACA Silicon Valley and is actively involved in other professional activities. He is a Chartered Accountant, CPA, CISA and a CRISC.

Kartik Trivedi, Partner and Co-founder, Symosis

Kartik Trivedi is a partner and co-founder at Symosis with 15+ years of experience helping numerous entities including Fortune 500, non-profit, tech start-up, financial services, and healthcare organizations meet their security, privacy, and business needs by helping to define strategic goals, develop road maps for more functional, mature, and secure programs, address immediate issues, and drive implementation of practical security solutions. Prior to Symosis, Kartik was director of application security at Accuvant, Managing Principal at McAfee, and Principal at Foundstone and software development engineer at concept solutions. Kartik has MBA & MS Degrees and CISM, CISA, CISSP certifications.

Specialties:

- Security risk assessment, penetration testing and prioritize vulnerability remediation based upon risk exposure to the business
- Application and mobile IOS/Android security, cloud security, secure software development, threat modeling, code reviews
- PCI, HIPAA, ISO and other security standards and compliance requirements
- Security training for developers, technical management and all workforce - delivered On-Demand and instructor led
- Published author & regular speaker at OWASP, RSA, ISACA conferences

Stephen S. Wu, Silicon Valley Law Group

Stephen Wu of Silicon Valley Law Group advises clients on information governance matters, focusing on information security, privacy, mobile computing, electronic discovery preparedness, records management, and secure electronic commerce. He served as the 2010-2011 Chair of the American Bar Association Section of Science & Technology Law, and before that he co-chaired the Section's Information Security Committee. He wrote or co-wrote six books, including A Legal Guide to Enterprise Mobile Device Management: Managing Bring Your Own Device (BYOD) and Employer-Issued Device Programs published by the American Bar Association in 2013.

Sponsors

The companies listed here have contributed to the success of this conference in a number of ways. They have provided financial backing for the conference as well as some of the subject matter experts presenting here today. The ISACA - Silicon Valley Board of Directors thanks these companies and their employees for all of their support.

Platinum Sponsor: BPM

BPM ACCOUNTANTS & CONSULTANTS

BURR PILGER MAYER

BPM is a full-service accounting and consulting firm deeply experienced in assurance, tax, business consulting, and wealth management. With over 50 committed partners leading these groups, we deliver the resources, experience, and know-how of a Big Four with the responsiveness and accessibility of a regional firm.

Platinum Sponsor: SOAProjects

SOAProjects

Our professionals join us from the largest accounting firms in the Bay Area; and our team comprises full-time employees as opposed to contractors. We provide a wide-range of services and serve clients ranging from early-stage high-potential start-ups to high-growth pre-IPO companies to well-established Fortune-100. Since we focus on only hiring experienced managers, senior managers and partner-level professionals, this enables us to provide high quality work product and deliver significant value-add to our clients. We have a global foot-print with 15 offices in 10 countries around the world and headquarters located in Mountain View, California.

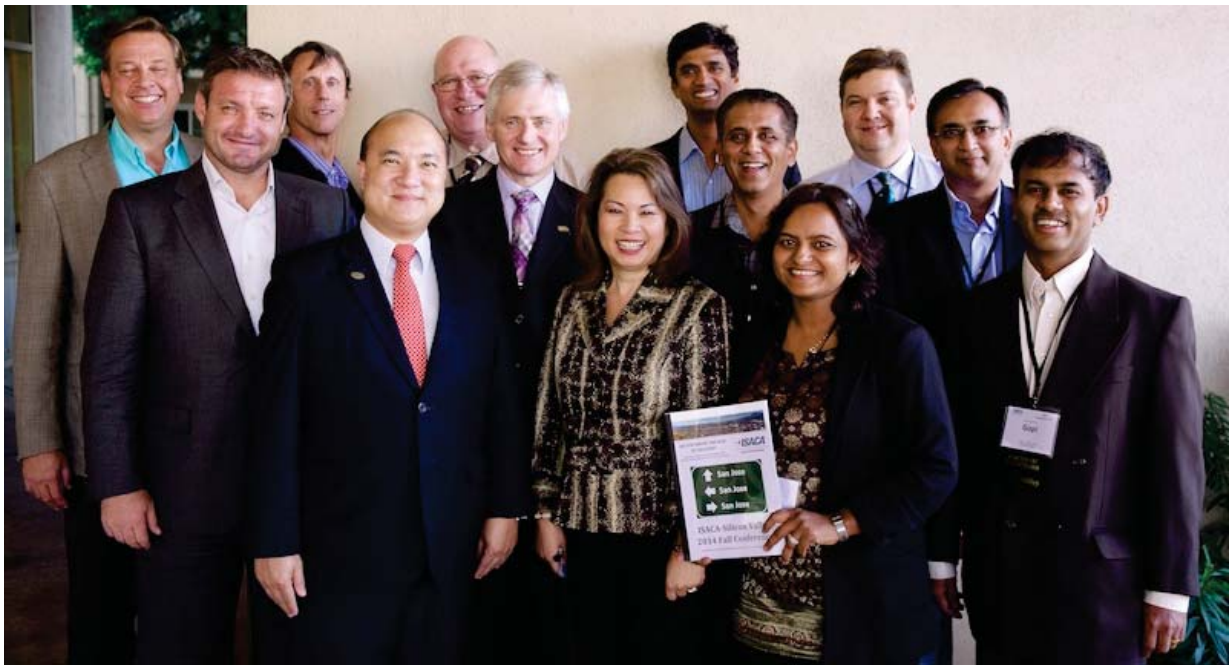
We are committed to bring the highest quality of service to our clients and strive to drive value and deliver industry best-practice improvements to each of our clients' business processes. In addition we assist our clients in meeting the project objectives efficiently and effectively. We focus on a forward-thinking model of providing end-to-end services and support the growth of our clients.

About ISACA & ISACA-Silicon Valley

ISACA is a nonprofit, global membership association for IT and information systems professionals. ISACA is committed to providing its constituency of more than 115,000 in 180 countries with the tools they need to achieve individual and organizational success. The benefits offered through our globally recognized research, certifications, and community collaboration results in greater trust in, and value from, information systems. Through more than 200 chapters, ISACA provides its members with education, resource sharing, advocacy, professional networking, and a host of other benefits on a local level.

ISACA-Silicon Valley is an award-winning Very Large Chapter started in 1982. We host monthly events that together offer over 50 CPEs a year, certification training, and networking opportunities to a membership of about 1,000.

For more information, please visit **www.isaca-sv.org**, write to the board at **theboard@isaca-sv.org** or give us a call at (650) 762-9478



ISACA-Silicon Valley Board and ISACA International Board at ISACA-SV Fall 2014 Conference

ISACA - Silicon Valley Board of Directors

Mike Jordan, President
Larry Halme, Vice President
Prasad Sanjeevaiah, Secretary
Rob Yewell, Treasurer
Ruchi Gupta, Conference Director
Naimish Anarkat, Academic Relations Director
Brijen Joshi, Membership Director
Bhupinder Singh, Certification Director
Gopi Ramamoorthy, Program Director
Murali Chandrasekharan, Marketing Director
Sumit Kalra, Past President