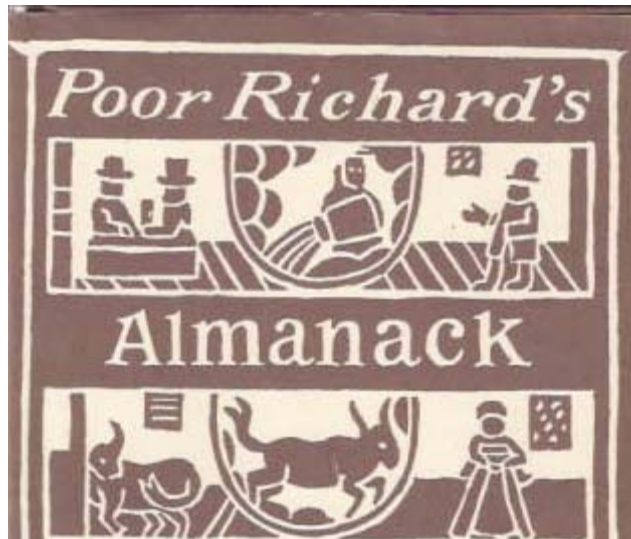


Presents

Hawaii's 16th Annual Discover Security Conference 2009



Doing More with Less

In Poor Richard's Almanack, Benjamin Franklin exhorted us to do more with less perplexity. But, one of his overall themes was just plain to conserve and "do more with less." As you know, current economic times suggest a similar theme. This year, ISSA Hawaii is proud to present our 16th Annual Discover Security Conference. We have a very impressive line up of Speakers and Exhibitors from almost all of the major Security Vendors. While many of the presentations will focus on how to optimize security and compliance in today's economy, some will focus on the latest information related to other topics related to Security and Disaster Recovery, such as PCI Compliance, Endpoint Security, the latest threats, botnets, ID Theft, and Data Loss Prevention.

When: October 14 & 15, 2009
(Registration begins at 7:30 am)

Where: Hale Koa Hotel – Honolulu, Hawaii



REGISTRATION FEE:

- ❖ **ISSA MEMBER: \$35.00**
- ❖ **NON-ISSA MEMBER: \$70.00**

ISSA Discover Security Conference 2009 Agenda

Day 1 – Wednesday, October 14th

7:00am – 8:00am BREAKFAST - Sponsored by LogLogic

8:15am – 8:30am **Welcome to Discover Security**
Kickoff William Musson

8:30am – 9:10am **Convergence of Log Management, Security Event Management and Database Security Management**
Speaker 1 Todd Cernetic
LogLogic

9:20am – 10:00am **Forward Architecting Your Security to Scale with Your Business**
Speaker 2 Michael Rothschild
Juniper Networks

10:00am – 10:30am BREAK / EXHIBITION

10:30am – 11:10am **Web 2.0 Exploits & Remediation**
Speaker 3 Anthony Blakemore
Accuvant

11:20am – 12:00pm **Redefining Network Security and Control**
Speaker 4 Bryan Wood
Fortinet

12:00pm – 1:00pm LUNCH - Sponsored by LogLogic

Speaker 5 **Manage by Measurement through a Control Framework**
Jerome Jackson
Technology Integration Group

1:00pm – 1:30pm BREAK / EXHIBITION

1:30pm – 2:10pm **Leveraging Cloud Technology to Maximize Security Information and Lower Log Collection, Monitoring & Correlation Costs**
Speaker 6 Lee Patenaude
Solutionary, Inc.

2:20pm– 3:00pm **Managing Availability: An Ounce of Prevention is worth a pound of Disaster Recovery**
Speaker 7 Duane Takamine
Secure Technology Hawaii

3:00pm – 3:30pm BREAK / EXHIBITION

3:30pm – 4:10pm **ID Theft: Technical Threats and Countermeasures**
Speaker 8 Beau Shahriary
Accuvant

4:20pm – 5:00pm **Is Your Payment Application Placing Your Company At Risk?**
Speaker 9 James Cowing
Digital Resources Group

5:00pm – 5:30pm EXHIBITION

Day 2 – Thursday, October 15th

7:00am – 7:45am BREAKFAST – Sponsored by McAfee/TIG

8:15am – 8:30am Day 1 Wrap Up and Day 2 Kickoff
William Musson & Jock Purnell

8:30am – 9:10am Intelligent Security and Compliance Optimization
Speaker 1
Adrian Cunningham
McAfee

9:20am – 10:00am PCI Compliance – Doing More with Less
Speaker 2
Cary Lynch
IBM/ISS

10:00am – 10:30am BREAK / EXHIBITION

10:30am – 11:10am Identity Awareness and DLP
Speaker 3
David Miller
CA

11:20am – 12:00pm Strategy for “Doing More with Less”
Speaker 4
Jeff Wells
Cisco Systems

12:00pm – 1:00pm LUNCH – Sponsored by McAfee/TIG

Working Smarter, not harder, in the Small to Medium Business
Speaker 5
Anthony Giandomenico
Secure DNA

1:00pm – 1:30pm BREAK / EXHIBITION

1:30pm – 2:10pm Advancements in EndPoint Security
Speaker 6
Michael Favinsky
CheckPoint

2:20pm – 3:00pm Changing the Economics of WiFi
Speaker 7
Clint Bogaard
Ruckus Wireless

3:00pm – 3:30pm BREAK / EXHIBITION

3:30pm – 4:10pm Death to passwords - Combining Strong Authentication and ESSO to Protect Your Information Assets at the Front Door
Speaker 8
Max Kellogg
Imprivata

4:20pm – 5:00pm Botnets and Oday Exploits: The Building Blocks of Today's Organized Internet Crime Syndicates
Speaker 9
Marc Eisenbarth
Tipping Point

5:00pm – 5:30pm CLOSING REMARKS / EXHIBITION
5:30pm – 7:30pm Refreshments and Luau Sponsored by McAfee/TIG

ISSA Discover Security Conference 2009

Speakers – Day 1

Improving Efficiencies through the Convergence of LOG Management, Security Event Management and Database Security Management

Speaker:

**Todd Cernetic, Regional Sales Manager
Loglogic**

Bio:

Todd has over 15 years of experience, strategic development in sales/marketing in the technology space. He has direct interaction with CEO, CIO, CISO, Vice President, Director contacts; Value Added Resellers and Purchasing departments in Hawaii, and the Southwest U.S.

Todd's overall expertise is not only in the security strategic technology business cycle but also in design, implementation and workflow production of IT security technology business models. He is also an active member in ISSA, ISACA, and INFRAGARD in Hawaii and Southwest U.S.

Todd has been a speaker for IDMA & ITVA Regional Conferences; DVD Demystified -Apple Seminar Series Nationwide, DVD Now; International Interactive Communications Society; DVD and the Web; Creative Labs-VARVision; ISACA; ISSA; National Assoc. of Broadcasters; National Religious Broadcasters; SANS, National Indian Gaming Assoc.; TribalNet; Angelbeat; HawaiiTechCon, Specialty Equipment Manufacturing Assoc and has been interviewed on KSUI-TV, KABC-TV, 760 KFMB talk radio in Southern California.

Todd is also an enthusiastic, Husband, Father, blues musician and long-suffering Chicago Cubs fan.

Topic:

Organizations face increasing threats to valuable enterprise data due to insider threats and external attacks, which are very real and require careful risk management. A database activity monitoring solution effectively integrated with a log management platform adds valuable business efficiencies to an organization's compliance initiatives, capitalizing on the logs it is already collecting. This integrated approach to compliance presents organizations with an opportunity to evaluate and enforce comprehensive policies and reporting structures across the IT infrastructure, including compliance requirements that range from detective controls, record retention, forensic investigation and log reviews. Using an open log management platform as a foundation, organizations can easily implement preventative measures that help assess the exposure and effectiveness of compensatory controls.

In this session you will learn about innovative ways of approaching database activity monitoring.

- * How the convergence of technology increases efficiencies
- * How to unleash log power to monitor database activity
- * How to create repeatable and improved business efficiencies

Mind the Gap – Forward Architecting Your Security to Scale with Your Business

Speaker:
Michael Rothschild
Juniper Networks

Bio:

Michael Rothschild has more than 17 years experience in marketing and product management for technology based organizations with specific focus in networking, security and compliance. At Juniper, he is responsible for driving the messaging and promotion of solutions that accelerate the delivery of high-value and converged applications that build differentiation and sustainable growth for enterprises. Prior to Juniper, Rothschild held senior management positions and has an established track record in launching a network security company, playing a key role in the IPO of a major VOIP company, and has been involved in the successful exits of two security companies. Rothschild is a Professor of Marketing at Yeshiva University in New York City and has published several works on marketing strategies. He holds an MBA in marketing and information systems and volunteers as a paramedic

Topic:

It was not all that long ago that security was relatively easy to deploy. The bad guys were on the outside, the good guys were on the inside. We simply had to build a protective perimeter around our own virtual fortress that separated the good guys from the bad.

And while approach worked with varying degrees of success, the design of the enterprise has changed as has the types of attacks targeting our business.

This session will peer into the world of hacking where we will discover the motivation behind many of the attacks, the physiology of a breach. We will discover the gaps in protection many organizations have because the playing field has changed. Once we understand these gaps we will discuss simple and very effective strategic and tactical ways to mitigate this unnecessary risk allowing us to chase business and not the hacker.

Web 2.0 Exploits & Remediation Strategies

Speaker:

**Anthony Blakemore, Principal Security Consultant
Accuvant**

Bio:

Anthony Blakemore has been a senior security consultant with Accuvant since 2008. Blakemore's security consulting experience included enterprise security posture reviews, FISAP audits, PCI QIRA investigations, information security policy creation, incident response analysis and procedural design, and hardened host configuration reviews. He is involved in code reviews and penetration testing, and helps augment the assessment practice's capabilities by designing and developing security tools.

Before joining Accuvant, Blakemore worked as a security consultant and project lead at Neohapsis, where he conducted penetration tests, vulnerability assessments and application assessments against business critical applications and architectures for dozens of Fortune 500 and multiple Fortune 100 companies. Blakemore holds a Bachelor of Science degree in Computer Science from DePaul University.

Topic:

Is your organization using Web 2.0? More businesses are, whether they know it or not. Familiar sites that now contain user-generated content are just one of the changes that Web 2.0 has brought to the workplace. A recent survey of 1300 IT professionals found that 95 percent of businesses allow access Web 2.0 in the workplace, but a surprising number lack the necessary security to protect against the unique threats it can introduce. Join Accuvant for this informative discussion on Web 2.0 Technologies and the threats inherit to them. Accuvant will dive into an in-depth discussion showcasing Web 2.0 security vulnerabilities and will share solutions for remediating potential Web 2.0 threats. Session topics include:

- Demonstration of the most prominent Web 2.0 security attacks
- Know how to assess and mitigate Web 2.0 threats
- Strategies for implementing Web 2.0 protection

Redefining Network Security and Control

Speaker:

Bryan Wood, Fortinet

Bio:

Several years experience in the networking and network security industry. Current role is managing the Western Channel Team from Minnesota out to the Hawaiian Islands. Previous experience includes:

- 3COM Corporation (Business Development Manager VOIP Technology)
- WatchGuard Technologies (Territory Manager) - UTM company
- NitroSecurity (Regional Sales Director) - IPS company
- Fortinet (Manager, Western Channel Sales).

Topic:

Redefining Network Security and Control

- The Evolution of Network Security
- Consolidation Drivers - Slowing growth of IT budgets, reduction in footprint, dynamic threat landscape
- Can we do more with less?
- Latest technologies that will keep us secure in the future

Manage by Measurement Through the Use of a Control Framework

Speaker:

**Jeromie Jackson, Senior Security Architect
Technology Integration Group**

Bio:

Jeromie Jackson is a highly sought after security & governance consultant. His entrepreneurial spirit had allowed him to build two successful security VAR & consultancies since 1994. Mr. Jackson is the President and founder of the San Diego Open Web Application Security Project (OWASP) Chapter, Vice President of ISACA San Diego, and a SANS Mentor. He obtained his CISSP in 1996, and also holds CISM, COBIT, and ITIL certifications. He is a speaker at many conventions, been interviewed on several radio talk shows, and was covered on Forbes Magazine. Today Mr. Jackson continues to consult enterprise and SMBs on measuring and improving their information security, risk management, and governance.

Topic:

Operational costs and regulatory burdens yield little value to most IT executives. We will focus on leveraging a best-practice framework based on the principals of IT and business alignment, risk management, resource management, and managing by measurement. By taking a top-down portfolio approach to risk management participants will be able to clearly communicate their value to the organization.

Attendees will:

- Learn how to simplify the burdens of overlapping regulations
- Learn how to develop leading and lagging indicators
- Become familiar with the Control Objectives for IT (COBIT)
- Take away steps to start managing and documenting their value to the organization

Leveraging Cloud Technology to Maximize Security Information and Lower Log Collection, Monitoring & Correlation Costs**Speaker:**

**Lee Patenaude, Technical Sales Support Lead
Solutionary, Inc.**

Bio:

Currently the leader of Solutionary's technical sales support team, Lee Patenaude provides a depth and diversity of security expertise. Lee is extremely well versed on all aspects of network security, and Solutionary's resident expert on application security. Lee brings a wealth of both technical hands-on security experience -- understanding the operational challenges of security, and the business drivers and business challenges associated with security.

Lee's background includes:

- Vice President, Worldwide Customer Services at Breach Security
- Lee was a founder of Breach Security in the US
- VP Sales & Services, Gilian Technologies
- Responsible for the worldwide sales organization as well as the systems engineering/customer support team
- Manager, BMC Software Consulting
- Technical Manager, New Dimension Software
- Data Center Manager, Burlington Northern
- Manager of Data Center Operations, BAX Global

Topic:

Log Monitoring – Leveraging cloud technology to maximize security information while minimizing the costs associated to log correlation and analysis. This presentation will cover how organizations can increase their knowledge of malicious security activity, meet compliance regulations, and leverage security best practices while limiting their investment for acquisition and maintenance of additional infrastructure.

Managing Availability: An Ounce of Prevention is worth a pound of Disaster Recovery

Speaker:

**Duane Takamine, CCISP, RSA, VCP
VP/CTO, Secure Technology Hawaii**

Bio:

Mr. Takamine is one of the co-founders of Secure Technology Hawaii, currently in its 16th year of providing expert security & disaster recovery solutions to Hawaii, CONUS, and the Pacific Rim. Mr. Takamine is a senior systems engineer designing, deploying, and supporting numerous enterprise solutions to most of Hawaii's top 250 firms. In his role he manages projects, provides training to the technical team, performs forensics and advanced technical support, and is a regular speaker on technology topics throughout the year.

Topic:

A significant percentage of the total cost of ownership of IT infrastructure is the cost to respond to various outages and disasters of different scales. Disaster Recovery and Business Continuity Planning generally attempt to moderate those costs by implementing strategies to deal with problems when they occur. But many of the technologies and strategies used to recover from disasters can also be used to prevent them, or reduce their magnitude when they occur. This presentation will cover strategies to integrate disaster prevention with disaster recovery to make a more holistic approach to improving IT resource availability while reducing the cost of maintaining them at the same time.

ID Theft: Technical Threats and Countermeasures

Speaker:

**Beau Shahriary
Managing Consultant, Accuvant**

Bio:

Beau Shahriary is a managing consultant with Accuvant's assessment team. Shahriary has more than a decade of experience in computer security consulting. He has performed security assessments, security remediation and strategic planning for a host of Fortune 500 companies. Shahriary's primary experience is in firewalls, secure network design and implementation, Microsoft security, modem security, wireless networking, and strategic security planning. His core competency is in conducting security assessments and creating a strategy to help clients meet today's secure network requirements based upon the HIPAA and GLBA regulations and ISO-17799 best practices.

Prior to joining Accuvant, Shahriary worked for Foundstone as the Senior Managing Consultant and project manager for the professional services group.

Shahriary is a Certified Information Systems Security Professional (CISSP), a Certified Checkpoint Security Administrator (CCSA), and a Microsoft Certified Systems Engineer (MCSE)

Topic:

Identify theft continues to soar and the risk of consumers losing personal data is at all time high. This in-depth discussion will share various methods and sources that contribute to the harvesting of personal identifiable information and provide countermeasure strategies to prevent data leaking and identify theft from occurring.

- A Growing Problem
 - Identity Theft Reported Statistics
 - High Profile Incidents
- Analysis of Current & Common Attack Vectors
 - Reconnaissance Activities
 - Identity Verification
 - Phishing
 - Spyware/Malware
 - Corporate High Value Assets
- Countermeasures
 - User Awareness
 - IT Security
 - Technology Solutions

Is your Payment Application Placing Your Company at Risk?

Speaker:

**Jim Cowing, CISSP, QSA, PAQSA, CISM, CPA, CITP
CEO/Managing Director – Digital Resources Group**

Bio:

James Cowing is a CISSP, QSA, PAQSA CISM, CPA, CITP and CEO/ Managing Director of Digital Resources Group (DRG), a QSAC and an ASV for PCI. Over the last 12 years, Mr. Cowing has helped industry leading financial institutions, merchants, and service providers address the complex and stringent IT security and compliance requirements of the Payment Card Industry, as well as conduct controls reviews such as ISO17799, HIPAA and GLBA. As the former co-chair of the Security Committee for the Financial Services Technology Consortium (FSTC), and a member of ISACA, ISSA, InfraGard and the American Institute of Certified Public Accountants (AICPA) Information Technology Division, Mr. Cowing is a seasoned professional and an experienced speaker in the payments, controls and security industries.

Topic:

Is your Cash Register, PinPad, Web Shopping Cart, or Point of Sale system secure? Are these often neglected applications the weakest link in your network infrastructure? Many companies are finding that the applications they use to interface with customers and handle all their monetary transactions can be placing their company at grave financial and legal risk.

When using computer applications that handle, process, or store consumer information, the importance of information security cannot be overvalued for any successful business. However, many companies today unknowingly place their company at risk by using third party payment applications that store personally identifiable customer information or prohibited cardholder data, such as full magnetic stripe, CVV2 or PIN data; or payment applications that lack essential security controls.

In an effort to strengthen the fragile ecommerce industry and shore up this gaping hole in the payment process, the PCI Security Standards Council last year announced the addition of the PA-DSS (Payment Application Data Security Standard). A year later, PA-DSS requirements and the implication for non-compliance are still widely misunderstood.

In this interactive session, attendees will learn:

- Common payment application exploits (including SQL injection, cross-site scripting and other OWASP top attacks)
- What PA-DSS is, who must comply and by when
- How PA-DSS can minimize payment application vulnerabilities
- What security guidelines exist for unattended payment terminals (UPTs), hardware security modules (HSMs) and PIN pads
- What type of penalties and fines can non-compliant companies incur
- How to set priorities and effectively manage PCI compliance programs

ISSA Discover Security Conference 2009

Speakers – Day 2

Intelligent Security and Compliance Optimization

Speaker:

Adrian Cunningham, McAfee

Bio:

Adrian Cunningham has been a Sales Engineer for McAfee since 1998, providing over 10 years experience as a Security Sales Engineer. He initially began selling McAfee security and PGP encryption software and has since become well versed in firewalls, vulnerability scanners, NAC and IPS. As a McAfee employee he's helped maintain full accountability for executing pre-sales technical sales support to corporate, state/local government and channel accounts. He also developed and prepared in-depth technical training to sales engineers at channel partner accounts and McAfee sales reps, and provided evaluation support for customers. Other real world experience comes from work as a security administrator for a 2500 employee operation as the firewall, HIPS and network IPS administrator.

Topic:

During this discussion, Adrian will describe how to approach the many business security needs we see today in the workplace from the global landscape. He will also discuss NIST best practices to protect against the latest threats and perform a hacking demo. The demo will show just how easily cyber criminals can still break in to even a well-secured network.

PCI Compliance – Doing More with Less

Speaker:

Cary Lynch, IBM

Bio:

Cary Lynch's current position is an Engagement Manager and is focused on the overall delivery responsibilities for ensuring the successful delivery of multiple projects from initiation to closure. It includes oversight of customer engagements including project management responsibilities, customer satisfaction, contract and scope reviews, invoicing requirements, financial/revenue tracking and obtainment. This role includes the management of multiple engagements at one time. Prior to Cary's current role, her background includes over 9 years within the Information Security industry with focus in information security assessments, including policy development based on several industry frameworks, security

architecture reviews, vulnerability identification and exploit, social engineering tests, physical security reviews, PCI audits and consulting at all PCI merchant and service provider levels. In addition, Cary has focused her efforts on security technology implementations and configurations such as IDS/IPS, scanning software and firewalls.

Topic:

1. Brief PCI overview and how it applies to all merchants (large and small)
2. Consequences of no action
3. The reality of limited IT budgets
4. What IBM has recommended (examples) of compensating controls that have helped companies achieve compliance w/out breaking the bank
5. What IBM recommends for maintaining PCI compliance (in a cost effective manner)

Leveraging Identity Awareness to Focus Your Data Loss Prevention Efforts

Speaker:

David Miller, CA, Sr Director, Security Product Marketing

Bio:

David Miller leverages over 15 years of experience in product management and marketing for security, compliance and CRM enterprise software solutions to understand customer needs and promote security awareness. For CA, David manages the product marketing efforts for the CA DLP (Data Loss Prevention) product line. In this capacity, he frequently speaks at security and privacy conferences, meets with customers, and works to ensure that the CA DLP solution reflects the customer needs of today and tomorrow while meeting and exceeding pertinent regulatory requirements. David's area of focus is data loss prevention, but he works closely with other CA Security solutions including Access Control, Identity Management, and Enterprise Log Manager. David holds an M.B.A. in marketing and strategy, and B.S. in Electrical Engineering.

Topic:

Data Loss Prevention, or DLP, is a topic that is receiving significant attention within the information security community as individuals and organizations realize the importance of managing and protecting sensitive information. The impact of a breach can be significant, resulting in lost productivity, financial penalties, and business-impacting negative exposure in the press.

Historically, the biggest challenge facing companies working to address this risk is determining when a specific action actually represents a breach of data security policy. Solutions that provide a single set of rules or policies applying to all employees are forced to manage to the lowest common denominator, so that legitimate business activity is not disrupted. Oftentimes, this results in organizations being reduced to monitor for simple data elements, such as social

security numbers or credit card numbers, crossing the Internet network boundary.

In order to overcome this challenge and effectively implement a data security solution, security organizations need to deploy an identity-aware DLP platform. These solutions tie together an understanding of the individuals involved in an action with the data involved in the action to determine, with a higher level of accuracy, whether the action should be allowed.

In this presentation, Steve will detail the benefits of identity-aware DLP and provide representative examples from industry of how identity-aware DLP has allowed organizations to realize previously unknown levels of accuracy.

Strategy for Doing More With Less

Speaker:

Jeff Wells, Security Specialist, Cisco Systems

Bio:

Jeff Wells, Security Specialist, Cisco Systems. Involved in IT since late 1970s, over 30 years programming experience, 25 years of analog and digital data networking experience, and over 15 years experience in IT security disciplines. CCIE and CISSP, 8 years as Cisco SE and consulting SE focused on security solutions and best practice.

Topic:

1. Focus on risk - this is an economic move, stop spending money where there is little or no risk mitigation. Give up on "check boxes".
2. Focus on management – more effective tools can give you force multiplication; poor management tools can actually increase costs.
3. Focus on scale – virtualization and centralization of resources can allow you to do way more with what you already have.

Working Smarter, Not Harder in the Small to Medium Size Business

Speaker:

Anthony Giandomenico, CEO of Secure DNA

Bio:

Anthony K. Giandomenico is the Founder and CEO of Secure DNA. He is involved with all aspects of business operations at Secure DNA and is in charge of strategic direction setting and innovation. He has significant experience in intrusion detection and firewall technologies, incident response procedures, security assessments and integrating various technologies. He has served as a media consultant to various media outlets in the area of information security and has been recognized as a leader in Hawaii's business community, receiving numerous awards including recognition as one of Hawaii's Top 40 business people under the age of 40 in 2007. Mr. Giandomenico has held various industry certifications and currently holds a GCIH

Topic:

Purchasing an IT asset may seem like a trivial cost on the surface, but dig a little deeper and over time you will realize that trivial cost is just the tip of the iceberg. Once purchased that asset needs to be deployed securely, configured with applications, patched and let's not forget that those assets are used by humans so add on the hours of support! And as the list of daily tasks continues to grow the funding to support those tasks becomes less. How can we keep up?

The Answer? Having the right information to make educated decisions. Join Anthony K Giandomenico as he provides us with keen insight on fully understanding the trials and tribulation of the IT lifecycle.

Advancements in EndPoint Security**Speaker:**

**Michael Favinsky, CISSP, Security Engineer
Check Point Software Technologies**

Bio:

Michael Favinsky has been involved in network and data security for over a decade. Based in Los Angeles, California, Mr. Favinsky has provided infrastructure and handled security threats for nearly all of Hollywood's global entertainment and media corporations. As a consultant, he also performed security implementation, project management, and incident handling in the e-business, financial, telecom, publishing, and manufacturing industries. Mr. Favinsky currently serves as a Security Engineer for Check Point Software Technologies. Mr. Favinsky holds a Bachelor of Science in Computer Science from the California State University, as well as several networking and security certifications.

Topic:

While most security projects and solutions focus on the network or perimeter, the endpoint and end-user are often neglected. Despite our best efforts, social engineering, insider theft, unawareness, and accident are responsible for some of our most visible and costly losses. In today's presentation, Mr. Favinsky will discuss the social, political, and technical aspects of endpoint security and show how to easily overcome these challenges by securing the endpoint.

Changing the Economics of WiFi**Speaker:**

Clint Bogard, Western Region Manager

Ruckus Wireless

Bio:

Clint has been working in the network space for the past 20 years starting his career with 10BaseT. Clint spent 14 years in the network infrastructure arena, a couple years in the consulting services arm of Intel and joined Ruckus in 2008. Clint has a BS in Compute Science and is responsible for Ruckus business in the western US and western Canada.

Topic:

A look at how Ruckus Wireless is changing the economics of WiFi. This will be a discussion about "where the puck is going" in regards to WiFi and user mobility. We'll also talk about how wireless (and 802.11n) 'changes the game' regarding edge switching requirements and cabling investments. Clint will include a brief overview of the Ruckus ZoneFlex enterprise WiFi solution including both indoor and fully hardened outdoor WiFi equipment. If you are looking to migrate to 802.11n, don't miss this presentation.

Death to passwords - Combining Strong Authentication and ESSO to Protect Your Information Assets at the Front Door

Speaker:

**Max Kellogg, Western Regional Director
Imprivata Inc.**

Bio:

Max Kellogg has been at the forefront of best of breed Enterprise Security for over 10 years. Prior to joining Imprivata, Max ran the Western US for Aventail's SSL VPN Appliance Line (acquired by SonicWALL) for over 3 years. Max also has extensive experience in Enterprise Email Security with a combined 7 years with IronPort Systems (acquired by Cisco) and Sendmail Inc. Max is based in the San Francisco Bay Area where he lives with his wife. When not traveling the West evangelizing leading edge security solutions, Max enjoys piloting his Cessna, Fly Fishing and enjoying the occasional bottle of California Wine.

Topic:

In recent years, enterprise single sign-on (ESSO) has emerged as an easy, smart and affordable way for organizations of all types and sizes to strengthen IT security while supporting user productivity. With the advent of more stringent government regulations, organizations are seeking ways to further strengthen IT security by incorporating stronger passwords and in many cases an additional form of authentication, such as a security card or token or even finger biometrics. The idea behind using an additional factor beyond a password provides strong authentication so that each computer on an organization's network has a stronger "front door" against entry by unauthorized users. However, the use of these increased security measures has an impact across the organization, both on all computer users as well as the helpdesk staff who need to support these

users. ESSO alleviates the inconvenience not only of a multiplicity of stronger passwords to access applications, but also integrates with strong authentication to ensure that every "front door" in the organization is as secure as possible. But which authentication option is right for you and your organization? And how easily can it be integrated with your ESSO solution? These are just two of the many questions to consider as you evaluate strong authentication choices. This topic explores these questions and addresses how organizations can achieve strong authentication with ESSO — easily and affordably — to increase their security levels dramatically without creating inconvenience for either IT staff or end users.

Botnets and 0-day Exploits: The Building Blocks of Today's Organized Internet Crime Syndicates

Speaker:

Marc Eisenbarth, Tipping Point

Bio:

Marc Eisenbarth is a Security Researcher within the Digital Vaccine group at TippingPoint. Some of his many interests include attack event visualization, botnets research, and honeynet analysis. Before joining TippingPoint, Marc completed a Masters degree in Computer Science at Columbia University, taking advanced courses in intrusion detection, cryptography, and machine learning. Marc also has 5 years experience in the Aerospace and Defense industry serving on both incidence response and enterprise security architecture teams.

Topic:

The profile of hackers has changed dramatically over the last few years into an extremely sophisticated and economically motivated body of attackers. Zero day exploits and botnets are used to construct multi-tiered distribution networks, which rival today's enterprise networks in complexity and resiliency. The scale of attacks has also escalated from a simple sale of zero day exploits on the black market to "one-stop-crimeware" web application packages with around the clock technical support. This talk will begin by outlining the current threat landscape and then focus in on the role that zero day exploits and botnets play in today's organized Internet crime syndicates. The speaker will use data from TippingPoint's Zero Day Initiative and ThreatLinQ security intelligence portal to show the evolving role that zero day exploits and botnets will continue to play in the world of organized Internet crime.

Menu – Days 1 & 2

Breakfast Day 1 – DeRussy Hall

- ❖ Assorted Muffins
- ❖ Assorted Danishes
- ❖ Coffee, Decaf, & Tea
- ❖ Fruit Juice

Sponsored By:



Lunch Day 1 – Banyan Tree Showroom

- ❖ Appetizer: Hale Koa Salad with Tarragon Dressing
- ❖ Main Course: Grilled Flank Steak and Broiled Mahimahi Filet
- ❖ Served on Spicy Fried Noodles and Sautéed Zucchini with Tomatoes
- ❖ Dessert: Vanilla Ice Cream Taco with Fruit

Sponsored By:



Breakfast Day 2 – DeRussy Hall

- ❖ Assorted Muffins
- ❖ Assorted Danishes
- ❖ Coffee, Decaf, & Tea
- ❖ Fruit Juice

Sponsored By:



Lunch Buffet Day 2 – Banyan Tree Showroom

- ❖ **Appetizer: Hale Koa Salad with Tarragon Dressing**
- ❖ **Main Course: Broiled New York Steak**
- ❖ **on Roasted Garlic Mashed Potatoes with Cabernet Peppercorn Sauce,**
- ❖ **Frizzled Onions, Grilled, Marinated Squash and Peppers**
- ❖ **Dessert: Tropical Cheesecake**

Sponsored By:

McAfee®

Afternoon Break Day 1 & 2 – DeRussy Hall

Sponsored By:

McAfee®

Reception/Luau Day 2 (5:00 pm) – Luau Garden

Sponsored By:

McAfee®

The splendor and spectacle of an ancient Hawaiian tradition comes alive at the Hale Koa Luau! As you enter the tropical garden, you are greeted with a lei and taken back to an old Hawaiian setting of thatched hale (houses) that protect guests from the misty rain, but keeping the outdoor ambience.

A Hawaiian musical duo and lei making demonstrations will keep you entertained during cocktail hour. Experience an authentic imu (Hawaiian underground oven) ceremony followed by a bountiful feast of authentic local flavors. Our sumptuous menu includes native delicacies such as lomi lomi salmon, kalua pig, teriyaki beef, shoyu chicken, Mahimahi, fresh fruit, pineapple and poi. At twilight, our spectacular luau show hosted by international recording artist Glenn Medeiros, will take you on a musical journey through the islands of Polynesia. Including the graceful hula and a live fire knife dance!



Luau

5:00 p.m. – 6:00 p.m. Bar Service Available
6:00 p.m. Dinner Served