
## Monday, July 11, 2011

| | |
|---|---|
| 4:00 pm - 6:00 pm | **Registration Open** |
| 5:00 pm - 6:00 pm | **Welcome Reception** |

## Tuesday, July 12, 2011

| | |
|---|---|
| 7:00 am - 5:00 pm | **Registration** |
| 7:00 am - 8:00 am | **Breakfast** |
| 8:00 am - 8:10 am | **Opening Remarks**<br>Jerry Archer, CISSP, Senior Vice President and Chief Security Officer, Sallie Mae<br>Bob Bragdon, Publisher, CSO magazine |
| 8:10 am - 9:30 am | **RISK AND METRICS SESSIONS** |
| 8:10 am - 8:30 am | **Value Illumination with Risk Management**<br>Jamil Farshchi, CISO, Los Alamos National Laboratory<br><br>This presentation will provide a high-level overview of the Value Illumination Strategic Security Model. This model ties together strategy, budget and security controls -- by virtue of quantitative risk management -- to create a streamlined information security program. |
| 8:30 am - 8:50 am | **Designing, Developing and Implementing an IT Vendor Assurance Program**<br>Vincent Campitelli, Vice President, IT Risk Management, McKesson Corporation |

Management, McKesson Corporation In this session, learn how McKesson created a program to quickly identify those IT vendors that provide products and services that could pose various degrees of risk to McKesson, along with the remediation plans to manage and monitor the associated risks.

8:50 am - 9:10 am **Metadata and Visualization: New Tools for Managing Complex Problems**
Kurt Neumann, Senior Manager, Security Engineering, Intuit

A proliferation of security tools, mass aggregates of data, and analytical requirements have made maintaining situational awareness difficult. This talk will cover the emergence of new tools and concepts to help reign in some of those risks.

9:10 am - 9:30 am **Info Security's Perfect Storm – Security Requirements for 2011 and Beyond**
Ray Wizbowski, Senior Director, Marketing & Communications, Global, Gemalto

The year 2011 is quickly becoming the "year of the breach." With financial institutions, online networks, and even a security company announcing they were compromised, we need to take a serious look at security requirements -- especially policies and practices that cover who is able to access what parts of the corporate network. Identity is the cornerstone of this conversation, and we'll explore it in this talk.

9:30 am - 10:00 am **Networking Break**

10:00 am - 12:00 pm **HUMAN FACTORS SESSIONS**

10:00 am - 10:20 am **Ethics in the Workplace**
Kevin Smith, Vice President, Sallie Mae

The root cause of internal theft or employee misconduct is a matter of ethics. This session will focus on the need for security representatives to become engaged with employee training programs, and help mold the ethical behavior of employees in the workplace. Attendees will come away from this session with specific examples of how to build a workplace ethics program.

10:20 am - 10:40 am **Integration Challenges of Acquisitions**
Mary Ann Davidson, CSO, Oracle

Acquisition integration presents many integration challenges, among them enforcing consistent secure development and assurance standards and creating a community of product security excellence. If "supply chain" is the current "cri de coeur," then "security assurance compliance" is one of the key answers to the problem statement.

10:40 am - 11:00 am **Don't Forget the Guy in the Bright Pink Shirt**
Sean Cordero, Information Security Consultant, Cloud Watchmen

Information security tools continue to bolster the visibility into enterprises, but with this arsenal in hand are we effectively deploying these and if so have we ignored the obvious gaps? In this session, we'll provide a refresher on basic information security practices in the age of too many tools.

| | |
|---|---|
| 11:00 am - 11:20 am | **How IQT Can Help Fund Cyber Security Startups**<br>George Hoyem, Partner, In-Q-Tel |
| | In this session, we'll discuss how IQT can help these startups gain access to large intelligence community customers, and how intelligence community cyber security needs can help CSOs -- and visa versa. |
| 11:20 am - 12:00 pm | **The Cyber Espionage Threat – You are a Player**<br>Robert Bigman, CISO, U.S. Central Intelligence Agency |
| | Cyber espionage takes advantage of naïve, and often irresponsible, participants in a deadly serious game that many public and private organizations are not even aware they are playing. Cyber espionage must be a part of your information assurance defense plans. This presentation describes key issues you must consider and recommends a plan for cyber health. |
| 12:00 pm - 1:00 pm | **Networking Lunch** |
| 1:00 pm - 2:20 pm | **SECURITY TESTING AND BENCHMARKING SESSIONS** |
| 1:00 pm - 1:20 pm | **Top Website Vulnerabilities: Trends, Business Effects and How to Fight Them**<br>Jeremiah Grossman, Founder & CTO, WhiteHat Security |
| | Most websites were exposed to at least one, serious vulnerability every day of 2010. Only 16% of websites were vulnerable less than 30 days of the year overall. In this session, get a statistical picture gleaned from over five years of vulnerability assessment results taken from over 3,000 websites. |
| 1:20 pm - 1:40 pm | **Security Benchmarking**<br>Abe Kleinfeld, President & CEO, nCircle, inc. |
| | The time has come for all organizations to measure the performance of our security ecosystem using consistently measured, fact-based, objective metrics, in much the same way CFOs measure the financial performance of our companies. And also like CFOs, we must be able to compare our performance to that of our peers. Only in this way can we begin to justify our spending, performance, new investments and simultaneously raise the bar of cybersecurity protection in our insustries. This presentation will help organizations to get started right away with Security Benchmarking and Perfomance Management. |
| 1:40 pm - 2:00 pm | **Gray, the New Black: Gray-Box Web Vulnerability Testing**<br>Brian Chess, Founder / Chief Scientist, Fortify Software, an HP Company |
| | Penetration testers who use only black-box tools are destined to lose to attackers who are willing to spend more time or effort looking for vulnerabilities. Defenders need to make use of one of the few natural advantages at their disposal: ready access to the system they're trying to protect. In this talk, Brian will discuss gray-box vulnerability testing techniques that expose web application internals so that testers understand what an application is doing and can spot vulnerabilities faster. The tool for this kind of testing observes the program while it executes. It reveals attack surface, points out vulnerable program behavior, and opens up a code-level view of the application. |

2:00 pm - 2:20 pm **Testing Security Controls Before Hackers Do**
Tas Giakouminakis, CTO, Rapid7

While investments in security can reduce the likelihood of breach, sophisticated attackers will always find a way. In this threat environment, organizations must be prepared to not only prevent and detect attacks, but to have robust security response protocols. These protocols must be tested, refined, and maintained in order to be effective. In this session, we'll discuss techniques and approaches for testing and refining security response.

2:20 pm - 3:20 pm **IDENTITY SESSIONS**

2:20 pm - 2:40 pm **The State of the IAM SaaS Market**
Lyle Carlson, Partner, Edgile, Inc.

Over the past decade in-house IAM investments have often fallen short of expectations. As the sector matures, the return on IAM investments is becoming easier to achieve, though costs remains stubbornly high. Enter the IAM SaaS vendors, taking aim at the cost side of the equation. Please join us as we present an objective view of the IAM SasS market.

2:40 pm - 3:00 pm **Safeguarding User Access For Cloud Computing**
Darran Rolls, CTO, SailPoint Technologies

Cloud computing presents as many challenges as it addresses, particularly around security and governance. From the business perspective, managers think they're simply removing the middleman from the process. In reality, they could be providing unregulated access to important data without understanding the larger security implications for the company. Identity and access governance has emerged as a critical deployment requirement in order for organizations to benefit from this new way of computing. For each application that they deploy in the cloud, IAG provides the control and visibility of who "should", who "does" and who "did" have access to what.

3:00 pm - 3:20 pm **Identity: How Do I Know Who You Really Are?**
Don Adams, CSO, TIBCO Software

Many changes are underway across industry, government and e-commerce that will fundamentally change the how, who and why of identity. In this session, we'll cover just a couple of these topics -- like ICAM to NFC – along with the implications, risks and opportunities they represent.

3:20 pm - 3:50 pm **Networking Break**

3:50 pm - 4:10 pm **APPLICATIONS SESSIONS**

3:50 pm - 4:10 pm **What I *Really* Think: We Are All Gonna Die**
Brad Arkin, Senior Director, Product Security & Privacy, Adobe Systems

As the guy responsible for some of the most widely distributed (and therefore, widely attacked) software on earth, I've got an interesting

perspective on where the good and bad actors in the tech security world are moving. This talk is an off the record conversation about where the real security vulnerabilities are (hint: everywhere), where the economic incentives are taking us (hint: high investment in attacks, low investment in defense), and what it all means (hint: see the second part of the topic above). I'll provide a ray of sunshine at the end to wrap on a positive note.

4:10 pm - 4:30 pm **DNSSEC: A Game Changing Example of Multi-stakeholder Cooperation**
Richard Lamb, DNSSEC Program Manager, ICANN

The biggest improvement to the Internet's security infrastructure began last year with the deployment of security extensions at the top of the Internet's global phone book (DNS). Unbeknownst to most, this humble effort has laid the foundation for the world's first global PKI that will provide cross-organizational and transnational opportunities for authentication. In this session, we'll talk about how we got here, current status, and the implications this and parallel technologies have in our collective cyber security efforts.

4:30 pm - 4:50 pm **Why Does Only 30% of the Fortune 1000 Own DLP? Why Wasn't DLP a Huge Success?**
Jason Clark, Chief Security and Strategy Officer, Websense

Jason Clark has done extensive research on the DLP Business and searched to find out where did DLP go wrong. He will share insights of what he found and also share a vision for the future on Data Theft Protection.

4:50 pm - 5:10 pm **Next-generation Threat Protection: Stopping Advanced Malware, Zero-day and Targeted APT Attacks**
Ashar Aziz, CEO, CTO & Founder, FireEye

Advanced malware, zero-day and targeted APT attacks aggressively evade signature-based defenses and compromise the majority of today's networks. The primary mission for any organization dealing with advanced malware is integrating defenses to block known malware, stop outbound data exfiltration attempts, and detect zero-day, targeted attacks. In this session, Ashar Aziz will give five guiding principles for integrated, next-generation threat protection.

5:10 pm - 5:30 pm **Fending Off APT and Other Attacks**
Wolfgang Kandek, CTO, QUALYS

Current protection methods can't effectively block attacks, so we'll explore how to identify vulnerabilities on a continuous basis and how to implement a comprehensive mitigation and remediation program.

5:30 pm - 5:40 pm **Tuesday Wrap Up**

## Wednesday, July 13, 2011

8:00 am - 5:00 pm **Registration**

8:45 am - 8:50 am **Opening Remarks**

7:45 am - 9:30 am **SESSIONS ON THIRD PARTIES AND CUSTOMERS**

8:50 am - 9:10 am

**Know Your Customers**
Elon Ginzburg, Group Information Security Officer, Wells Fargo Bank

In this age of advanced persistent threats, banks are finding that their business customers are used as launching points, that everyone is on the front line, and knowing your customers is the next goal of layered security. When dual authentication is no longer a strong control, how can the enterprise use its customer knowledge to improve detection of possible fraudulent attacks? Find out in this session.

9:10 am - 9:30 am

**The Cat and Mouse of How to Hide and Track on the Internet**
Lance Cottrell, Founder and CTO, Anonymizer, Inc.

In this session, we'll explore the technologies people are using to hide their identities and activities, and how those may be overcome -- or at least detected.

9:30 am - 10:10 am

**MOBILE SESSIONS**

9:30 am - 9:50 am

**How Mobile App Development Upended Your SDL And What To Do About It**
Alex Stamos, CTO, iSEC Partners, Inc.

In this talk, we'll discuss the new challenges of mobile applications for application security and risk management teams, and offer a handful of mitigations to help manage this new risk. The talk will cover the evolution of the mobile application security model, a review of recent security incidents caused by mobile apps, and the technological lessons we can take from previous experiences with PC application development and the DRM problem. The talk will conclude with several vendor- agnostic recommendations for tools and techniques that can lessen mobile risk, and some predictions for how the mobile development paradigm will continue to shift our traditional notions of security and trust.

9:50 am - 10:10 am

**Mobile Security Can Be a Customer Delighter**
Dan Corcoran, Group Information Security Officer, Consumer Group, Intuit

While it may go against the conventional wisdom, mobile security can be a customer delighter and, when done right, can actually increase customer adoption of mobile applications that provide highly sensitive services such as finance, tax preparation, and health care. This discussion will address the challenges and opportunities to making this a reality.

10:10 am - 10:40 am

**Networking Break**

10:40 am - 12:20 pm

**CONTINUATION OF HUMAN FACTORS SESSIONS**

10:40 am - 11:00 am

**Responding to Insider Threats and Employee Defections**
Steve Kim, Managing Director, Stroz Friedberg

In this session, we'll discuss the security issues raised by insider threats to sensitive company data, plus how to manage the loss of data that frequently goes hand in hand with employee defections. Steve Kim, a leading expert in digital risk management and investigations,

will cover emerging security trends and various risks posed by company insiders. This insightful discussion will further explore the forensic evidence of digital theft that can often be uncovered in the wake of deceitful employee behavior. Steve will also address valuable strategies for mitigating disruptive damage caused by insider theft of intellectual property and other critical business information.

11:00 am - 11:20 am **The Cyber Security School Challenge**
Joyce Brocaglia, CEO, Alta Associates

The Cyber Security School Challenge is a collaborative outreach program founded by the EWF and in partnership with Carnegie Mellon University, the National Cyber Security Alliance and (ISC)2 to help educate our youth on the topics of cyber security and cyber bullying. We already have over 40 participants including teams from GE, Nationwide, Boeing and RSA. Who better than The Security Confabulation attendees to teach kids about cyber security, safety and possibly saving lives?

11:20 am - 11:40 am **Proposal for an Initiative Against Malicious Cyber Activity**
Donald Purdy, Chief Cybersecurity Strategist, CSC

This session will focus discussion and enlist support for an initiative by government and private sector representatives to create a business case, and develop and implement a plan to reduce the frequency, impact, and risk of malicious cyber activity -- including cyber crime, cyber terrorism, cyber attacks, and cyber warfare. The business case and plan should represent an understanding of, and strategic approach to, the ecosystem of malicious cyber activity that enables and rewards a continuum of malicious cyber activity -- from the relatively harmless hacker to the nation state and their proxies. The private sector is a key stakeholder in cyberspace and must be engaged in shining light on, and helping to address this problem set, not just as a victim and source of incident information. Although law enforcement is a key stakeholder as well, the problem requires engagement by all relevant government stakeholders.

11:40 am - 12:20 pm **Hummingbird: A Rotor Machine for the 21st Century**
Whitfield Diffe

Radio Frequency identification may not be growing fast enough to please its investors but remote management of ever smaller and cheaper devices is inevitable. Endless detail of the whereabouts, movements, ownership, status and intentions will be circulating freely on channels that are intentionally made easy to access --- after all, every two-bit tag has such a radio. The resulting cacophony will be mostly --- though not entirely: consider the manifest of a freight car full of drugs --- low-grade ore from an intelligence viewpoint but in aggregate, it will be of immense value. Our natural response is: lets just encrypt it. The rub is power. Standard cryptosystems like AES are power hogs even in implementations that put power first. The problem calls for a cryptographic algorithm that puts minimizing power consumption first: Hummingbird.

12:20 pm - 1:30 pm **Networking Lunch**

1:30 pm - 2:50 pm **COMPLIANCE/GOVERNANCE SESSIONS**

1:30 pm - 1:50 pm **GRC Optimization Over the Next 5 Years**
David Deckter, Partner, Edgile

GRC solutions need to evolve in order to keep pace with the evolving threat landscape. Unfortunately the vendors aren't evolving their products fast enough. And the auditors are holding back too. In this session, we'll discuss what the vendors and your auditors aren't telling you – and about the game changing strategies that must occur now to prepare your organization to take advantage of the next S-curve in GRC.

1:50 pm - 2:10 pm **Software Assurance in the Real World**
Ariel Silverstone, CISO, Expedia

In this session, we'll discuss how to put together -- and succeed in implementing -- a software assurance program.

2:10 pm - 2:30 pm **Payment Apps on Mobile and Tablet Devices are Cool – But Can They Be Trusted?**
Steven Elefant, CIO, Heartland Payment Systems

The proliferation of payment apps on mobile and tablet devices, e-wallets, and cloud services means more intermediaries accessing sensitive data and a wider dispersion of consumer and merchant data. While this gives consumers and merchants more choice for accepting and presenting payment, the security models are still emerging. Let's look at the risks and what old and new tools exist to help protect the security of the payments ecosystem on these new frontiers.

2:30 pm - 2:50 pm **Identity Theft and Online Fraud Protection at the IRS**
Hun Kim, Director, Online Fraud Detection and Prevention, IRS

This session will highlight increasing and evolving threats of online fraud and identity theft against taxpayers and will discuss proactive measures that the IRS is taking to prevent, protect, and respond to these threats, including victim assistance.

2:50 pm - 3:30 pm **Networking Break**

3:30 pm - 4:50 pm **CLOUD SESSIONS**

3:30 pm - 3:50 pm **Private Insecurities and Public Transparency**
John Collins, Senior Global Trust Product Manager, Google

The hype around cloud computing rages out of control as vendors rush to capitalize on the latest IT fad. "Private cloud" is a term that has appealed to IT security leaders as having the potential to offer all the benefits of the cloud (lower costs, ubiquitous access, etc) with none of the security risks. Both of these potentials are unrealized, despite vendor claims. This session will expose these assumptions and discuss why true cloud computing can offer significant security benefits over "private clouds" and legacy infrastructure.

3:50 pm - 4:10 pm **Moving Target Defense to Enhance Cloud Security**
Arun Sood, Professor, George Mason University

Intrusions are inevitable, and frequency of zero day attacks is increasing. Once in the system, the bad guys remain for days, weeks and months. In this session, we'll examine this problem by focusing on threat independent approaches that delete malware without detecting the malware.

| | |
|---|---|
| 4:10 pm - 4:30 pm | **Big Data: Big Security Risks**<br>Tim Mather, Industry Leader |
| | Cloud computing has ushered in the era of 'big data'. As organizations acquire more and more data, and need/want to use more and more of that data, the scalability of established relational databases is increasingly called into question. More and more, organizations are turning to distributed databases -- so-called NoSQL databases. However, the security provided for and by distributed databases is far short of what is available today to secure relational databases. With this shift to distributed bases, are organizations effectively setting themselves up for significant security problems? What can information security personnel do to make organizations aware of the specific issues? What compensating controls should we be considering? Learn more in this session. |
| 4:30 pm - 4:50 pm | **Understanding and Adopting Cloud Computing**<br>Bob West, CEO, Echelon One |
| | Corporations have several significant motivators to understand and adopt cloud computing as part of their basic infrastructure. However, most organizations haven't taken the time to understand what cloud computing is and the security issues associated with cloud environments. This presentation will provide an overview of cloud computing, discuss strategic adoption issues, and recommendations about how move forward in adopting cloud computing as a strategic technology asset. |
| 4:50 pm - 5:10 pm | **The Do Not Track Debate**<br>John Mitchell, Professor, Stanford University |
| | In this session, we'll discuss online third-party tracking, the Do Not Track debate, and the changing nature of web interaction. We'll explore how new tools can monitor web sites to see how they track users, with some interesting results. |
| 5:10 pm - 5:20 pm | **Wednesday Wrap Up** |
| 7:00 pm - 10:00 pm | **Dinner at the** Monterey Bay Aquarium |

## Thursday, July 14, 2011

| | |
|---|---|
| 7:00 am - 11:00 am | **Registration Open** |
| 8:15 am - 8:30 am | **Opening Remarks** |
| 8:30 am - 10:30 am | **INNOVATION SESSIONS** |
| 8:30 am - 8:50 am | **Succeeding in a Cyber World: The Natural Evolution of Cybersecurity**<br>Lt. Gen Harry Raduege, Center for Cyber Innovation, Deloitte |
| | Not too long ago, information security was viewed as solitary service within an enterprise information technology strategy. Firewalls, anti-virus, access control and intrusion detection were the buzz words of a technology focused view to deter the threats associated with |

explosion of the internet. Today the natural evolution from information security to cybersecurity has caused this once technology dependant view to integrate much more closely with other departments within an organization. It is difficult to mention information security without including privacy, compliance, and governance and information risk in the same discussion. This evolution has caused security and risk leaders to review their existing frameworks and leverage internal process to meet the rising requirements presented through domestic / international laws and regulations as well as the advanced persistent threats presented by nation states and cyber crime syndicates.

8:50 am - 9:10 am **Mission of the Security Innovation Network**
Robert Rodriguez, Chairman and Managing Principal, Security Innovation Network

The mission of the Security Innovation Network™ (SINET) is to advance innovation and enable global collaboration between the public and private sectors to defeat Cybersecurity threats. SINET increases awareness between builders, buyers, researchers and investors in the Cybersecurity domain, in particular the Defense Industrial Base and the Federal Government. SINET utilizes a top down - bottom up, mutually beneficial and trust based approach to accelerate innovation and increases business opportunities for both small and large companies.

9:10 am - 9:30 am **Projecting Security Waves**
John Muir, Managing Director, Security Innovation Network (SINET)

By studying the formation of security companies in very specific categories, you can see waves forming up in certain areas. How long does it take that wave to crest? What is the average lifecycle of a pure-play security company? Find out in this session.

9:30 am - 9:50 am **Counter-Insurgency in Cyberspace**
John Mills, Special Assistant for Cyber Information Assurance, DASD IIA, DoD CIO, Office of the Secretary of Defense

Although much of the cyber conflict focus has been on potential threat vectors from near peer, nation state competitors, the real de-stabilizing danger may be the cyber insurgent. Using classic counter-insurgency tenets, an outline on how to successfully deal with cyber insurgents will be presented.

9:50 am - 10:10 am **Why Not Voiceprints?**
Dan Miller, Senior Analyst, Opus Research

The use of mobile phones for payments and peer-to-peer transfers is growing globally. Security is a high visibility nightmare. And while fingerprints and iris scans have been proposed, why don’t we consider voiceprints as a factor for mobile payment authorization, user authentication or esignatures? Since it's a phone, then "Why Not Voice?"

10:10 am - 10:30 am **Next Generation Security Environment for the Financial Sector**
Peter Fonash, Senior Advisor for Cybersecurity, Federal Reserve Board

In this session, we’ll use the Department of Homeland Security’s recent paper on "Enabling Distributed Security in Cyberspace" as a starting point for discussing the attributes of a next generation cybersecurity environment.

10:30 am - 11:00 am **Networking Break**

11:00 am - 12:20 pm **SECURITY TESTING AND BENCHMARKING SESSIONS**

11:00 am - 11:20 am **Stop Admiring the Problem and Fix the Bugs**
Joel Scambray, Managing Principal, Cigital, Inc.

We know from measuring our customers' practices that industry isn't improving software security through assessment. While we continue to optimize source code review and penetration testing assessment techniques, both obtain only marginal coverage of applications and thus impart less value than perceived. Few organizations employ techniques to understand their applications' architecture & design and almost all prefer finding more bugs to remediation. It's time to stop admiring the problem and do what it takes to fix these security bugs!

11:20 am - 11:40 am **A Pragmatic and Verifiable Security Approach Based on Attacker Behavior**
Daniel Guido, Security Consultant, iSEC Partners

In this talk, we'll introduce an intelligence-driven approach to malware defense, focusing on attacker's capabilities and methods, with data collected from the most popular crimeware packs currently deployed in the wild. This analysis identifies the means by which exploits are developed and selected for use in malware campaigns, identifies defenses that are outside the capability of malware exploit writers to bypass, and helps attendees evaluate not just the exploitability, but the probability of a vulnerability being exploited. This study shows that, until exploits in the wild substantially advance in sophistication, only a few simple defensive tactics are required to protect users from such opportunistic threats. When evaluated by my methods and data, the value of existing security products and processes and the wisdom of existing security best practices are directly called into question. Instead, we'll offer a new way forward based on verifiable observations and defenses supported by intelligence.

11:40 am - 12:00 pm **The Expansion of Fraud Opportunities Beyond Banking**
David Hahn, Director of Information Security, Intuit

12:00 pm - 12:10 pm **Closing Remarks**
Jerry Archer, CISSP, Senior Vice President and Chief Security Officer, Sallie Mae
Bob Bragdon, Publisher, CSO magazine

12:10 pm **Conference Sessions Concludes**

1:30 pm **Golf at** Pacific Grove Golf Course **(2:15pm tee time)**