Sunday, April 15, 2012

1:00 pm - 5:00 pm

Defining Your Organization's Risk Appetite, Securing Funding, and Getting Stakeholder Support: a CSO Executive Communication Workshop
Paul A. Argenti, Professor of Corporate Communication, Tuck School of Business

As more and more security executives are tapped for direct accountability to boards and audit committees, so comes the need to communicate, negotiate and network expertly on that level. Have you and your security enterprise effectively identified your company's risk appetite at the most senior levels of your organization? Have you formally communicated an enterprise security plan at this level? And have you not only secured the appropriate budget, but developed effective business relationships with senior-most stakeholders? Join us for this executive-level workshop where you'll gather take-away tips, strategies and examples of not only how to do this for organizational and personal career benefit, but how to avoid the easily encountered and costly pitfalls along the way.

5:00 pm - 6:00 pm **California Wine Welcome Reception**

Monday, April 16, 2012

7:30 am - 8:30 am **Networking Breakfast**

Sponsored by RSA and Verizon Business

8:30 am - 8:45 am **Opening Remarks**

8:45 am - 9:30 am **Opening Keynote: Here's What the Future of Security Looks Like**
Hon. Dale Meyerrose, Major General, United States Air Force (Ret.) and the First Presidentially Appointed CIO for the U.S. Intelligence Community, now President, MeyerRose Group, LLC.

Simply building deeper cyber moats and higher cyber walls will not afford the protection CSOs need to safeguard their mobile-device extended networks. The future is a trusted cloud, purpose built to provide both security and performance that offers the best in traditional firewalls and virus protections but also provides constant monitoring and assigns trust factor scores on-demand and in real time. Learn more about the future of security in this session.

9:30 am - 9:50 am **The Realities of APT: Are We Distracted by What's Fashionable -- and Missing What's Even Worse?**
Ken Baylor, Vice President, Antifraud Strategy and Emerging Threats, Wells Fargo
Today's threat landscape can be difficult to judge at any given point in time, but what's emerging? How are botnets the threat of the future? Learn more from a top emerging threats expert in this session.

9:50 am - 10:10 am **The Critical Role of Developing a Good Security Strategy**
Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, Visa

Creating a good strategy is difficult, never happens by accident and always requires a process. Unfortunately, those are just a few reasons why many organizations get tripped up. Join us for this session as we examine the elements of good strategy, show examples of real-life good (and bad) ones, and discuss the strategic process that a good strategy requires.

10:10 am - 10:30 am **Building Cyber Defense Strategies for the Future**
Bob Bragdon, Publisher, CSO magazine
Ken Baylor, Vice President, Antifraud Strategy and Emerging Threats, Wells Fargo
Hon. Dale Meyerrose, Major General, United States Air Force (Ret.) and the First Presidentially Appointed CIO for the U.S. Intelligence Community, now President, MeyerRose Group, LLC.
Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, Visa
Join us as our panel of experts takes your questions.

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

11:00 am - 11:20 am **Securing the Increasingly Hybrid Enterprise**
Jim Reavis, co-founder, Cloud Security Alliance

Today's enterprise increasingly involves public clouds, private clouds and users of both. Add mobility to the mix, and there's a dispersal of apps, data, users and endpoint devices that is only complicating security's objectives. Understand how the Cloud Security Alliance sees the future of security given these realities.

11:20 am - 11:40 am **Is the Lack of Technology-Enabled Governance Creating a False Cloud Economy?**
Kevin Walker, Vice President and Assistant CISO, Walmart

While clouds are viable for certain business applications, much time and a huge chasm sits between the clouds we're building today and true utility computing that can enable a wide swath of business services tomorrow. Today, we're leaning on legal documents to leverage protections, but what we really need are technologies that are preventative instruments. What controls are providers putting around my services, and why don't we know what they are? Why do we often need to wait until our next audit to understand them? Join us for this session as we explore how governance is the third rail in cloud computing, and what need to be done to neutralize it.

11:40 am - 12:00 pm **Cloud Security's Future: How to Prepare**
Bob Bragdon, Publisher, CSO magazine
Jim Reavis, co-founder, Cloud Security Alliance
Kevin Walker, Vice President and Assistant CISO, Walmart
Join us as our panel of experts takes your questions.

12:00 pm - 12:30 pm **Securing the Future: A Fireside Chat**
Bob Bragdon, Publisher, CSO magazine

Varun Kohli, Director, Product Marketing, HP Enterprise Security Products

View HP Video

12:30 pm - 1:30 pm **Networking Lunch with Table Topic Discussions**

- **The Evolution of Fraud in a Shifting Web Terrain: Mobile Users, Multiple Devices, and Managed Services** Greg Reber**,** AsTech Consulting
- **Security Performance Management: Why it matters and how to measure it** Jim Acquaviva, nCircle
- **Intersection of Information Governance and Information Security** Ken Liao, Proofpoint, Inc
- **Enticing Security Best Practices** Andrew Wild and Andrew McDonnell, Qualys, Inc
- **Next Generation Access Governance: Convergence of Access Certification and Unstructured Data Usage** Marc Potter, Quest Software
- **Security in the Boardroom...Now What?** Steve Hall, Tripwire, Inc

1:30 pm - 2:35 pm **Track Sessions on CyberSecurity**

1:30 pm - 2:00 pm

The Big Lie: Vulnerabilities vs. Exploits
Brad Arkin, Senior Director, Engineering Security, Standards, Open Source and Accessibility, Adobe Systems Incorporated

Strategies for Securing an Uncertain Future
Michael Theis, Former Chief of Cyber Counterintelligence, National Reconnaissance Office, U.S. Department of Defense; now President,

Cyber-Insider Threat Solutions

The big lie perpetuated by software security vendors is that improving the security quality of your code will eventually get you to a "good enough" level of security. The reality is that non-trivial software will always have non-trivial bugs, many of which will have interesting security characteristics for bad guys. I will dazzle you with real world data that shows the only tactic that works is raising the cost of exploit creation or reducing the value of exploits once created.

How do you design a security strategy for a world of continuous technological surprise? This session will explore the three key ingredients that need to be baked in to any successful security strategy. Join us and gather forward looking ideas for mitigating insider threats, cyber espionage, cyber criminals, and more.

2:05 pm - 2:35 pm

Are We Missing the Point?
Shelley Stewart, Executive Director, Global Security, Cummins Inc.

Lost in the constant barrage of new and improved threats, it can become easy for an organization to miss the point. Simply put, you can deploy all the tools you want, but if they're not an effective part of how you do business, they won't have a meaningful effect. Join us for this session as an expert explains how they've integrated security to business process for maximum effectiveness.

A Tale of Two Theories
Dennis Devlin, AVP, Information Security and Compliance Services, The George Washington University

Historically, Fortune 500 companies and higher-education institutions have approached information security differently. Higher education was one of the earliest adopters of IP-based network computing and the ARPANET, and has always favored an open approach to encourage learning, teaching and scholarship. Their model began as "allow by default and deny by exception." Fortune 500 companies entered the Internet era after the Morris worm, malware and electronic fraud had already occurred. From the very start, their model was "deny by default and allow by exception." Over the past two decades, the two models have converged, and each camp has learned from the other. At the same time, universities have been dealing with bleeding edge BYOD (bring your own device) programs, mobile technologies, flat networks with demarcations at the edge, telecommuting, distance learning, and customer communities that change every semester. This session will trace how we got to where we are today, the lessons we have learned along the way, and how models tried and tested by higher education can be useful for the Fortune 500 too.

2:35 pm - 3:05 pm **Networking Break**

3:05 pm - 4:10 pm **Track Sessions on Cloud Security**

3:05 pm - 3:35 pm **Deadbolts Are Dead: The Legal Implications of Security in a Wireless Cloud Environment**
Joshua Konvisser, Partner, Pillsbury Winthrop Shaw Pittman LLP
Catherine Meyer, Counsel, Pillsbury Winthrop Shaw Pittman LLP

As information becomes the most valuable asset in our economy, and the repositories of that asset are de-linked from any physical location through wireless client devices and cloud based server and storage, notions of security tied to a particular device and/or place are becoming extinct. This session will focus on legal considerations of securing information as it moves about in the new reality. In particular, we will explore those areas where the law has fallen behind this reality, and those areas in which the law is trying to adapt. Key areas of consideration include: notions of jurisdiction; data security laws; how California and Massachusetts changed the world; challenges auditing a virtual data center; risk allocation; contracting with service providers; and insurance challenges.

Cloud Security: New Realities and Safer Strategies
Jeffrey Garonzik, Chief/Cyber Security Architect, Central Intelligence Agency

Today’s modern computing architectures with increasingly diverse endpoints combined with increasingly constricted budgets mean that organizations need to call their shots very carefully. The luxury of flexibility now yields to doing things in more common ways to maximize security, budget and effort. Join us for this session as we learn how to plan in this direction for better security in the future.

3:40 pm - 4:10 pm

The Pact: Avoiding a Challenging Cloud Services Experience
Bob Bragdon, Publisher, CSO magazine
Sean Cordero, President, Cloudwatchmen
Omar Khawaja, Global Product Management, Verizon Business

Cloud computing is sometimes painted as Faustian bargain where the customer gives up control of their most critical assets (data, IP) and places it in the hands of their cloud provider. In exchange they receive promises of lower-costs, speed, flexibility, and unlimited computing power that could enable them better serve their customers. But is this dark view a realistic depiction of cloud services? In this talk, we'll circumvent the abyss of issues that can consume a company moving into the cloud and provide, through an example, a methodology to prepare in advance for clouds and how to head off the related security challenges.

Will Your SLA Save You in a Cloud-Based World?
Mitch Jaffe, Director of Infrastructure, Tyco International

Everyone is going to the cloud, and most IT initiatives are managed by SLA's, but what do they really mean? If your data is in your data center and a provider fails to perform, you can often replace your provider fairly easily. But once you go to the cloud, can you ever go back? Will your SLA's save you? More importantly, have you ever really read the SLA from cover to cover? Join us for this session as we get preventative tips on using cloud SLAs wisely.

4:15 pm - 4:45 pm

New Technology Demonstrations

See lightning-round demonstrations of new security products and services.

4:45 pm - 5:15 pm

Shaping the Future
Jerry Archer, CISSP, Senior Vice President and Chief Security Officer, Sallie Mae

As we run headlong into the next generation of computing with clouds, how will the future of security be altered and what role and responsibilities do information security professionals have in shaping that future? What are the key areas of thoughtful debate and exchange that will inform today's decision makers? The cloud outcomes are ours to shape -- and success or failure will be laid at our doorstep. Join us as we explore the opportunities that await.

5:30 pm - 6:30 pm

California Dreamin' Networking Reception

Sponsored by: HP Enterprise Security Products

Tuesday, April 17, 2012

8:00 am - 9:00 am **Networking Breakfast**

9:00 am - 9:15 am **Opening Remarks**

9:15 am - 10:00 am **Opening Keynote: Can Information Security Survive?**
Alan Ross, Senior Principal Engineer, Lead Security Architect, Intel Corporation

This is the question facing organizations of all sizes, and for some the answer is changing the mission and scope of their IT security initiatives. In this session Malcolm will discuss Intel's new "Protect to Enable" information security strategy. Malcolm will examine the challenges of balancing Intel's business needs and growth, with managing and mitigating risks in enterprise security — and will focus on strategies for any company interested in bringing employee-owned devices into the IT environment.

10:00 am - 10:20 am **The Future of Customer-Facing Security**
Bryce Austin, CIO, Wells Fargo Business Payroll Services

Every security expert would prefer that we all use a complex password, a SMART card and a fingerprint scanner to authenticate ourselves. Every user would prefer they just walk up to their computer and it automatically knows who they are so they can immediately start working. Somewhere in the middle is where our industry currently stands, but exactly where in the middle is a matter of great debate. And where it should be in the future is an even greater debate. Join us as we explore the issue.

10:20 am - 10:40 am **Embracing a World of New Customer Expectations**
Bob Bragdon, Publisher, CSO magazine
Bryce Austin, CIO, Wells Fargo Business Payroll Services
Nils Puhlmann, CSO, Zynga
Alan Ross, Senior Principal Engineer, Lead Security Architect, Intel Corporation

Join us as our panel of experts takes your questions.

10:40 am - 11:10 am **Networking Break**

11:10 am - 11:25 am **Minimizing Risk While Maximizing Business Value in M&A, Partnerships and Joint Ventures**
Ahmad Douglas, Senior Business Leader, Business Advisory, Visa

As long as companies seek new capabilities and enter new markets, finance and legal departments will be arranging relationships between firms. Mergers, acquisitions, partnerships, joint ventures and other arrangements hold out the promise of new value for the company. But these relationships can also bring new risks into the equation. Is your information security program prepared to contribute on this critical front? Does it even have a seat at the table? In this session, we'll examine these relationships, and the value case for including information security as a core participant in the process of deciding whether to enter into them. We also discuss the acquisition process, walking through each step, identifying key pain points and offering a holistic strategy for minimizing new risk while maximizing business value from the relationship.

11:25 am - 11:40 am **Adaptive Risk Monitoring**
Jeff Recor, Senior Manager, Deloitte & Touche LLP

11:40 am - 11:55 am **Reducing Risk Through Next-Gen Cyber Awareness Training**
Dan Lohrmann, CSO, State of Michigan

Training and awareness are critical to heading off security threats. But generating active participation and understanding is a massive hurdle.

How are organizations finding new ways to overcome the obstacles? Join us for this session as we see how the State of Michigan has elevated the message and participation among it’s 50,000 state employees.

11:55am - 12:10 pm

I'm Telling Mom On You
Mary Ann Davidson, CSO, Oracle

"I'm telling Mom" survives childhood altercations as a useful management technique with applicability in the corporate security world. Ideally, we implement security broadly and resolve security issues at the lowest level, as everyone does his security bit. However, despite our best training, motivational techniques and "engagement," sometimes we need to "rat out" a group or organization that is not getting with our security program. How and when do you do this? And, how do you grab senior management's attention so that they take needed action - and fast? Lastly, how do you engage the sinners, so they not only repent and sin no more, but go forth and convert the heathen?

12:10 pm - 12:30 pm

Getting in Front of Risk With New Thinking
Bob Bragdon, Publisher, CSO magazine

Mary Ann Davidson, CSO, Oracle
Ahmad Douglas, Senior Business Leader, Business Advisory, Visa
Dan Lohrmann, CSO, State of Michigan

Join us as our panel of experts takes your questions.

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

1:30 pm - 2:35 pm **Track Sessions on Consumerization and Mobile Security**

1:30 pm - 2:00 pm

Bring Your Own Device Programs: Avoiding Pitfalls and Developing Policies
Michael R. Overly Esq., Partner, Foley & Lardner LLP

Bring-your-own-device programs are the new craze, fueled by user demands for versatile and popular devices, along with perceived cost-savings by CFOs. But the common pitfalls when implementing these programs are emerging. In this session, get expert advice on how to develop an effective BYOD policy and how to identify often overlooked issues.

This Will Only Get More Difficult Until...
Nils Puhlmann, CSO, Zynga

Today's challenges with enabling a mobile workforce have little to do with the devices, and everything to do with data, usage and managing expectations around a rapidly advancing and widely adopted, multipurpose tool. Nonetheless, corporate and institutional viewpoints and policies are not only grasping to find their way, they're ranging from rigidly conservative to fleetingly progressive. Faced with a shortage of talent and innovation, today's security field is unprepared for all of us. Join us for a unique view of the current state -- and seasoned insights on where we need to go.

2:05 pm - 2:35 pm

Staying ahead of the Security Poverty Line with Mobility and the Cloud
Andy Ellis, Senior Director of Information Security and Chief Security Architect, Akamai Technologies

Whether it's mobility, cloud, or general IT security, operating below the security poverty line isn't about budget, it's about attitude, motivation, and focusing not simply on basic compliance but rather on your true security goals. Akamai's security program evolved through the collapse of the dot-com bubble, avoided being trapped below the security poverty line, and developed into one of the most trusted cloud platforms today. See how Akamai CSO Andy Ellis plans on taking the next leap with mobility to stay far above the poverty line.

Balancing Innovative Mobile User Experiences and Data Protection and Privacy
Bob Bragdon, Publisher, CSO magazine
Kevin DePeugh, Executive Director, Security, Kaiser Permanente

For some organizations, smaller form factors like handhelds and tablets create significant productivity enhancements across large sectors of the workforce. And while striking a balance between the best possible user experience and ensuring that sensitive data is protected can be a challenge, there are proven ways to find the optimum service delivery. In this session, see how Kaiser Permanente has embraced mobility and addressed cutting-edge use cases for its inherently mobile clinicians.

2:35 pm - 3:05 pm **Networking Break**

3:05 pm - 4:10 pm **Track Sessions on Governance, Risk and Compliance**

3:05 pm - 3:35 pm

How to Deal with a Global Regulatory Landscape: A Methodology

BAE Systems' Journey to Successful Risk Management

for CSOs
Bob Bragdon, Publisher, CSO magazine
Richard Kelly, Director of Global Security, Ingersoll Rand
Shukri Khader, CISO, Avon Products

Global companies face compliance with a slew of global privacy and data protection laws. The challenge is further magnified when some laws conflict with one another. For example, companies are required to protect certain kinds of information, thus requiring them to deploy tools to identify the information, yet this very action may be in violation of another set of laws. Join us for this session as we discuss an approach to navigate through some of these conflicting laws in order to protect the enterprise while simultaneously meeting global regulatory requirements.

Eric Noonan, CISO, and General Manager for ETS, BAE Systems

As CISO of an organization with 90,000 employees, Eric Noonan knows that the secret ingredient to successfully managing risk at the executive committee level is engaging with the business. Join us for this session as he describes how his security and risk organization takes a risk management, not risk avoidance, approach and how this has enabled a global security assessment that the business embraces and supports.

3:40 pm - 4:10 pm

Balancing the Art and Science of Risk Management
Bob Bragdon, Publisher, CSO magazine
Kevin DePeugh, Executive Director, Security, Kaiser Permanente
Dick Parry, Executive Director, Global Security, Novartis Institutes for BioMedical Research

Operational risk management can be fraught with tangled, overlapping toolsets, a false sense of coverage, and competing business expectations. That said, other disciplines of the business seem to successfully develop clear objectives and measure results in a quantitative fashion. So why does security and risk management have to be any different? Join us and learn more about how to balance the art and science through logical integration of risk control strategies.

The Future of Risk Management
Eric Cowperthwaite, System Director of Enterprise Security and CSO, Providence Health & Services

Risk, opportunity and reward are critical to business success. Every CEO, CFO and COO knows that. If that's so, why don't we see robust risk management programs? When will see them? What will they look like? In this session, we'll take a look at a forward looking model to create a robust program.

4:10 pm	**Conference Concludes**