Thursday, March 21, 2013

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

9:00am - 9:15am **Welcome and Opening Remarks**
Bob Bragdon, Publisher, CSO magazine

9:15 am - 10:00 am **The New Normal of Cybersecurity: Adapting the Role of Government**
Andy Ozment, Senior Director for Cybersecurity, National Security Staff, The White House

The intensified threat of cyberattacks on critical infrastructure -- and the real consequences created by advanced persistent threats -- is changing the security game. This new normal is reshaping ideas about the government's role in cybersecurity, and drawing its capabilities and limitations into sharper focus. In this session, the White House's Senior Director for Cybersecurity, Andy Ozment, will discuss the federal government's current thinking on the respective roles of the public and private sector. He'll also outline the Administration's cybersecurity priorities, the goals of President Obama's recently-enacted Executive Order 13636, and how CSOs can participate in addressing security gaps and reducing risks.

10:00 am - 10:30 am **APT Protection Via Data-Centric Security**
Alan Kessler, President and CEO, Vormetric

The APT tornado is getting larger, is gathering speed, and we're all in its path of destruction. Perimeter security and simple encryption don't cut it. Perimeter security is irrelevant when the threat is inside, while simple encryption gives a false sense of security since it lacks the policy control to protect against privileged

user exploitation. Moreover, while many believe that compliance equals safety, it doesn't. "Check box" security may give comfort, but like a placebo, it offers limited real protection against today's sophisticated cyber-attacks. As the APT landscape evolves, the risk to valuable data is always present, so enterprises need to take a data-centric protection approach, adding defense layers around the very thing that matters most: sensitive data. Join us as we discuss the best ways to reduce the attack surface of APTs and that yield high-value security intelligence.

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

11:00 am - 11:30 am **Security as Offense: Moving from Advanced Persistent Threats to Advanced Persistent Security**
Gregory T. Garcia, Principal, Garcia Cyber Partners

Disarming today's security threats before they do damage takes superior defenses. But today's enterprises can't overlook the importance of a good offense. In this session, Greg Garcia, principal at Garcia Cyber Partners and member of the federal government's Information Security and Privacy Advisory Board, shares key tactics designed to help organizations establish proactive "Advanced Persistent Security," or around-the clock, proactive monitoring and management based on the notion that attacks have already infiltrated the perimeters. Greg will outline critical steps government and the private sector can take to work together, share sensitive but relevant information, and establish a collective knowledge base -- all in an effort to aggressively mitigate security risks and vulnerabilities.

11:30 am - 12:00 pm **CyberSecurity Confab Sessions**

Join us for this lightning round of 15-minute, rapid-fire presentations designed to inform and educate on a variety of cybersecurity challenges and solutions.

Connecting Security to the Business

Rod Murchison, VP of Products, Tripwire, Inc.
Now that information security is a boardroom topic, how can CISOs show value to their organizations in meaningful ways? In this session, Ron Murchison, VP of Products , shares techniques to elevate security strategies and tactics in a way that demonstrates greater business value, makes it easier to defend and acquire resources, and contributes to the success of your organization.

Business Implications of the Executive Order for Critical Infrastructure

Lamont Orange, Director of Information Security and Strategy, Websense, Inc.

This order will not only define standards for designated organizations, but additionally set a complementary direction for the companies doing business with them. Join Lamont Orange, Senior Director-Security for Websense, and the former CISO of Charter Communications, to hear how this direction will cascade through the vendor/business partner community and the threat protection and intelligence industries.

12:00 pm - 1:15 pm **Networking Lunch with Discussion Tables**

Reducing Cost with Employee and Customer-Facing Security Services
The risks related to identity fraud and data loss, along with the challenges of assessing each transaction, often inhibit organizations from realizing the cost savings of bringing critical services online. Join us as we

discuss how to confidently bring more services online while simultaneously managing risk.

Sponsored by CA Technologies

Driving Operational Efficiencies Through Privileged Access
Today's enterprises are motivated to find operational efficiencies -- often by leveraging data center consolidation, lowering the cost of resources and licenses, and increasing staff productivity. Yet consolidation presents new challenges in the form of multi-tenancy and disappearing physical boundaries — all of which beg the need for alignment of objectives between system administrators and application administrators. At the same time, privileged access can be a pivotal tool in this process. Join us as we discuss privileged access, and related strategies to create better efficiencies and alignment.

Sponsored by CA Technologies

Cloud Security Controls: Methods and Best Practices

When deploying application workloads to a remote cloud environment, security is naturally a critical consideration. While one key factor is the operational security of the cloud service provider, another is the layered deployment of logical security controls. What are the best practices for maintaining defense-in-depth security? Join us as we share examples of common control deployments and how they are often implemented in cloud environments.

Sponsored by Savvis

1:15 pm - 1:45 pm

Understanding and Mitigating Cybersecurity Risks: A Legal Perspective
Deen Kaplan, Partner, Hogan Lovells

CSOs know all too well what keeps them up at night. But those worries may not always consider the broader concerns of their constituents, including the CEO, CFO, directors, other business executives — and, of course, customers . In this session, Deen Kaplan, who counsels businesses and governments on a range of cybersecurity matters, will offer practical insights into the legal and regulatory obligations CSOs and their business executive peers face daily. Join us to get up-to-date advice on the legal and regulatory roles and obligations around your incident response team, your organization's data, and how it — and your

organization — can and should be protected.

1:45 pm - 2:15 pm

Cybersecurity 101 for CISOs: How to Smooth Out Your Uneven Security Posture
Bob Bigman, Former CSO, Information Assurance Group, U.S. Central Intelligence Agency; President, 2BSecure

While a wealth of products and services exist to mitigate enterprise cybersecurity risks, many organizations are unknowingly leaving doors wide open by not addressing the basics. In fact, the strongest IT security strategies start with fundamentals, including reading and following recommendations in technical documentation, using secure Unix OSes, and correcting settings on network routers. Without continued monitoring of these basics, your organization is left with an uneven security posture that expensive solutions might not even mitigate. Join us as Robert Bigman offers critical advice on cost-effective security basics that can serve as a foundation for wisely managed, additional investments.

2:15 pm - 2:45 pm

Networking Break

2:45 pm - 3:15 pm

Understanding and Protecting Against the Multiple Faces of Insider Threats
Randy Trzeciak, Technical Staff, Software Engineering Institute's (SEI) CERT Program, Carnegie Mellon University Cylab

While advanced persistent threats and cyber attacks from external sources make headlines, insider threats continue to quietly expand the perimeter of threats to organizations. That said, many organizations tend to lump all insider threats in one bucket -- and then build defenses based on that approach. In this session, learn about the distinct types of insider threats – from IT sabotage to intellectual property theft to fraud – and learn best practices to detect, protect against and act on each type. CERT senior member Randy Trzeciak will convey the "big picture" of the insider threat problem, share insights from the extensive library and comprehensive database containing hundreds of actual cases of insider cybercrime developed by The Insider Threat Center at CERT, and discuss the technical and behavioral aspects of actual compromises.

3:15 pm - 4:00 pm

A Whole of Nation Approach to Cybersecurity Response, Mitigation, and Recovery
Larry Zelvin, Director, National Cybersecurity and Communications Integration Center (NCCIC), U.S.

Department of Homeland Security (DHS)

The DHS' National Cybersecurity and Communications Integration Center (NCCIC) operates at the intersection of the network defense, private sector, civilian, law enforcement, intelligence, and defense communities. As a world class cybersecurity and communications organization, it performs cutting edge analysis and shares actionable and comprehensive information in real time. Join us for this session to learn how the NCCIC operates and the threats it mitigates on a daily basis.

4:00 pm **Closing Remarks and Seminar Concludes**
Bob Bragdon, Publisher, CSO magazine