Defending the Fortress: New Threats Meet New Defenses

Produced by CSO

THE SECURITY STANDARD™

September 13-14, 2010
Marriott Brooklyn Bridge, New York, NY

Monday, September 13, 2010

8:00 am - 8:00 pm	**Registration**
8:00 am - 9:00 am	**Networking Breakfast and Security Showcase**
9:00 am - 9:15 am	**Welcome and Opening Remarks**
	Bob Bragdon, Publisher, CSO magazine
9:15 am - 10:00 am	**Opening Keynote: Keeping on Top of Evolving Threats**
	Gary Lynch, Global Leader of International Trade and Supply Chain Risk, Marsh Inc.

It's an evolving world – and an ever-evolving "threatscape" with which you have to contend. Staying on top of the latest technological security concerns like securing storage and applications in the cloud, new Botnets, rootkits and phishing scams, as well as physical security threats like defending against disgruntled former employees and the forces of global terrorism, is a huge challenge. But security risk is not the only risk that organizations are managing as part of their enterprise risk initiatives. It's an exciting time to be managing security risk and now that security is back on the board room agenda the primary question becomes "How do CSOs keep security risk front and center when competing with so many other risk initiatives such as product, quality, environmental, supply chain, and health risk?" This session will provide a perspective on trends in gloabl risk management and the linkages with security risk initiatives, detail warning signs that your program might be "at risk" and demonstrate methods for how to keep the CSO agenda relevant and in sync with the Directors and Executive Officers agenda.

10:00 am - 10:45 am   **Safeguarding the Fortress: The Relationship between Global Threats, Threat Actors, Your Business, and Things You Can Control**
Richard A. Gunthner, Vice President, Global Corporate Security, MasterCard Worldwide
Roland Cloutier, Vice President and Chief Security Officer, ADP

Richard Gunthner, CSO of Payment Services giant MasterCard, and Roland Cloutier, CSO of Payroll Services giant ADP, provide a unique look into the intersection of technology with crime, fraud, and the global security issues that threaten your businesses and employees every day. These two experts will provide insight to a complex world of threats, controls, threat actors, and intelligence — all of which cross the boundaries between cyber protection and the physical world. Through discussion and demonstration of real world incidents, detection techniques, and everyday control capabilities, Richard and Roland will provide tangible techniques that will help you build and defend your corporate fortress.

10:45 am - 11:15 am	**Networking Break and Security Showcase**

11:15 am - 11:45 am **Now Moving to the Corner Office: The Business Value of Software Security**
Roger Thornton, Founder & CTO, Fortify Software
Bob Bragdon, Publisher, CSO magazine

In today's social, mobile and cloud oriented world, attacks are becoming more and more sophisticated — and this is shifting the complexity of security challenges across the organization. With this shift, security concerns are now finding their way into CEO offices and board rooms, causing some CSOs to report to the highest levels of management. With accountability to so many business leaders, how does the CSO communicate the value of the least understood aspect of security — software security? In this keynote presentation, Fortify's Founder and CTO Roger Thornton will discuss how today's security leaders across industries — from financial services to insurance to communications to government and defense — are tracking and communicating the ROI on securing code in mission-critical applications. Join us to learn more about how CSOs can communicate ROI in terms that all business leaders will not only understand, but appreciate.

11:50 am - 12:30 pm **Security Showcase Classroom**
Discover what's new, as sponsors each have a 10-minute open forum to educate attendees on current technologies and future solutions.

Mobile Phone Software Verifies Valid Credentials for Online Purchases
Presented by: Jim Reno, CTO, Arcot Systems
ArcotOTP is a software application that runs on a mobile phone and generates a one-time-password (OTP) used to authenticate to online applications and verify valid credentials for online purchases. With ArcotOTP, customers no longer need to carry a separate authentication token. ArcotOTP supports multiple OTP algorithms including those specified by OATH (HOTP/TOTP) and EMV (CAP/DPA). ArcotOTP provides strong authentication at a lower cost of ownership while increasing security and convenience for customers.

How Identity and Context Virtualization Fuels Enterprise Social Networking Initiatives
Presented by: Dieter Schuller, Vice President, Radiant Logic
Cisco recently embarked on an initiative to internally deploy Cisco Pulse -- a powerful new way to harness the collective expertise of the workforce that makes it quick and easy for employees to find the people and information they need to get their work done. To meet their business requirements in this case, Cisco needed to allow employees outside of the sales organization to access information from within Salesforce. For example, an employee in accounting might need to search for a salesperson (directory) along with a list of accounts they are responsible for (Salesforce). In this session, learn how Identity and Context virtualization technology was used to build a rich user profile from internal and cloud based identity sources enabling the Cisco Enterprise Social Networking deployment to meet its business requirements.

Leveraging Software Security Assurance to Build Trust in the Software You Use
Presented by: Jon Gettinger, Vice President, Fortify Software

Software Security Assurance (SSA) is a holistic approach to software security aimed at making applications more secure by addressing security risks in software code and preventing their introduction throughout the application life cycle. This discipline enables you to build trust in the software you depend on by helping you find, fix, and secure applications in less time and cost than perimeter-based methods or tool-centric strategies. This session will describe how SSA, along with the right people, processes and technologies, solves today's application security issues and will highlight how organizations can easily get started with a program to identify and reduce software risk.

IT Security + Fraud Management = Enhanced Authentication Efficacy
Presented by: Eli Katz, Vice President of Enterprise Strategies, Finance, 41st Parameter
Collaboration between IT security and fraud investigations can yield insight into ways in which crime rings attack and defeat an organization's authentication controls. Collaboration is particularly effective because so many offline frauds are proceeded by online fraud-staging events. This session will describe current attack profiles and how cooperation between IT Security and Fraud Management can implement simple yet extremely effective online "tripwires" that will benefit both organizations' performance.

12:30 pm - 1:30 pm	**Lunch**	
1:30 pm - 2:10 pm	**The Cloud Standard: Business Track**	**The Cloud Standard: Technology Track**
1:30 pm - 2:10 pm	**Assessing Security in the Cloud** Warren Axelrod, Research Director for Financial Services, United States Cyber Consequences Unit	**Securely Filtering Cloud-Delivered Data** Michael Theis, Executive Director, Cyber Threat Strategies, Raytheon

Whether your organization uses — or plans to use -- software or infrastructure hosted by third party providers, keeping your data secure will be one of your top priorities. Learn how to conduct rigorous due diligence of cloud providers -- from the security of their data centers to their tiers of infosec protection to the contractual terms that are must-haves. Whether you have or plan to use software-, platform- or infrastructure as a service, you won't want to miss this session.

Explore the cutting edge tactics, techniques and procedures being developed and implemented to securely filter cloud-based services for advanced persistent threats, zero-day exploits and social engineering attacks targeted at your sensitive intellectual property.

2:15 pm - 2:45 pm	**Increasing Operational Efficiency with a Governance Risk and Compliance (GRC) Framework** Sam Curry, Vice President, Product Management and Strategy, RSA, The Security Division of EMC Jerry Archer, CISSP, Senior Vice President and Chief Security Officer, Sallie Mae

Without a Governance, Risk and Compliance (GRC) Framework, organizations have a difficult time getting their arms around their governance, risk and compliance strategies. In this session, learn how Sallie Mae's senior leadership not only achieved improved situational awareness with their GRC framework, but also discovered key operational efficiencies.

2:45 pm - 3:15 pm	**Networking Break & Security Showcase Classroom**

Discover what's new, as sponsors each have a 10-minute open forum to educate attendees on current technologies and future solutions.

Data Loss Prevention: Managing and Protecting Confidential Corporate Data
Presented by: Richard Trezza, DLP Solution Architect, McAfee
Given today's strict regulatory environment, Data Loss Prevention is one of the most critical issues facing IT management. Employees today have many avenues to electronically expose sensitive data and the scope of this data problem can actually be greater than the threat from outsiders. You are likely losing confidential data without even knowing it, making a high performance, intelligent DLP solution a must for today's organizations.

3:15 pm - 3:55 pm	**The Cloud Standard: Business Track**	**The Cloud Standard: Technology Track**
3:15 pm - 3:55 pm	**Contracting with Your Cloud Computing Provider: The Legal**	**Trust but Verify**

Pitfalls You May be Overlooking
Christopher Wolf, Partner, Hogan Lovells

Vincent Campitelli, Vice President, IT Risk Management, McKesson Corporation

Standard service agreements don't go far enough in protecting your data and your organization in the event of security incidents or outages at cloud providers. In this session, learn how to negotiate the right terms and penalties to get the protection you need from your cloud provider, from identity management to business continuity, incident response plans and more.

So you're happy with your SaaS or cloud infrastructure contract and your providers' supposed guarantees. Should you stop there, or do some verification of your own? What are the rules around trying to break into your providers' systems or hiring a third party to do some monitoring so you can find out some of the activity hitting their perimeter? Learn what's accepted practice when you don't have access to your providers' logs but want assurance that events aren't going unnoticed.

4:00 pm - 5:25 pm	**The Digital ID World Standard: Business Track**	**The Digital ID World Standard: Technology Track**

4:00 pm - 4:40 pm	**Business-Driven Identity Management** Jerry Archer, CISSP, Senior Vice President and Chief Security Officer, Sallie Mae	**Identity Management: Obscured by Clouds?** Michael Theis, Executive Director, Information Protection Management Strategies, Raytheon Information Systems Security

As public companies work to address a growing list of compliance requirements, their IT organizations must partner and collaborate with the business on both the strategy and implementation of an identity and governance framework. In this session, you'll hear actionable advice about how to best engage business managers to create sustainable compliance processes for identity management.

There are three major challenges to successful identity management in the cloud: Accurately judging trust, right-sizing permissions, and effectively monitoring. We will discuss and demonstrate some of the proven techniques in assuring those three areas are successful and secure in any enterprise.

4:45 pm - 5:25 pm	**Identity Management Process Design** Steve Jensen, Vice President and Chief Information Security Officer, Carlson Wagonlit Travel	**Ten Steps to Transition Security Applications to the Cloud** Thanh Ngu, IT Senior Manager, Avago Technologies

Effective identity and access management comes from deploying the right technology and embedding IAM processes throughout the organization. In this session, learn how to develop an effective IAM

The path to using cloud security services -- like identity management, among others -- may not always be clear. To reap the benefits, organizations need to first carefully identify applications that can benefit from the efficiencies of the cloud, and then lay the groundwork to

strategy across your organization, no matter how siloed, geographically dispersed or decentralized your operations are.

succeed. In this session, hear how one organization did just that by successfully transitioning their major security applications to the cloud -- and then found immediate results on their bottom line. You'll also hear about ten key steps you can take to do the same for your own organization.

5:30 pm - 6:30 pm	**Networking Reception and Security Showcase**

Sponsored by:

6:00 pm - 8:00 pm	**Emerging Solutions Demo Presentations**

Filling security gaps is more important than ever as risks faced by organizations grow more varied and complex each day. Modeled after IDG's successful DEMO events, companies showcasing and judged in this session are given just five minutes to demonstrate how their product fills a critical need, and another 10 minutes of Q&A from our panel of judges -- just the companies, the technologies and the judges. Join us for this rapid-fire session as we cut right to the chase.

Judges: **John Kirkwood**, VP and Global Information Security Officer, Ahold; **Paul De Graaff**, Global Information Security Officer, AIG; **Warren Axelrod**, Research Director for Financial Services, The United States Cyber Consequences Unit; **Derek Slater**, Editor in Chief, CSO magazine

Tuesday, September 14, 2010

8:00 am - 4:30 pm	**Registration**
8:00 am - 9:00 am	**Networking Breakfast and Security Showcase**
9:00 am - 9:15 am	**Welcome and Opening Remarks**

Bob Bragdon, Publisher, CSO magazine

9:15 am - 10:00 am   **The Global State of Information Security: An Exclusive Survey Preview**

Bob Bragdon, Publisher, CSO magazine

Mark Lobel, Partner, PricewaterhouseCoopers

Join us for this exclusive preview of the industry's pre-eminent, annual survey on security -- the 2011 Global State of Information Security, conducted by CSO magazine and PwC. You'll learn how your peer security executives are focusing their spending in this climate and what their top priorities are for the coming year — along with a range of other trends critical to securing the corporate fortress.

10:00 am - 10:45 am   **The Growing Privacy Challenge: Aligning Privacy and Security to the Governance Framework**

Nuala O'Connor Kelly, Senior Counsel, Information Governance and Chief Privacy Leader, GE

As states across the country adopt legislation designed to protect personally identifiable information, organizations must put rigor into their policies, practices and training to ensure compliance. In this session, hear how GE approached the privacy challenge from the chief privacy officer on down, plus how it governed the areas where privacy and security meet.

10:45 am - 11:15 am   **Networking Break and Security Showcase**

11:15 am - 11:45 am   **Creating Continuous Risk Improvement Through the Next Decade**

Francis D'Addario, Security Executive Council Emeritus Faculty, Strategic Influence and Innovation, Former Affiliation: Starbucks Coffee Company

History proves that cataclysmic risk is inevitable -- whether it comes from natural or man-made disaster, or is brought about by malicious attack. Preparing for risk -- and minimizing exposure -- requires acceptance that readiness is a board-level priority. The board's security initiatives then need to be mapped against the strategic plan so that risks are considered over both the short and long term. The Security Executive Council's Security 2020 initiative aims to continuously improve risk and security measures industry-wide by providing security executive leadership training, advancing technology innovation through test beds, and creating a trusted process that examines how technologies can interoperate. Learn more about what the Security Executive Council's research is finding — and how this initiative can help you — in this session.

| 11:45 am - 12:15 pm | **Embracing Disruptive Innovation Without Friction: Security for the Next-Generation Workforce** |

Embracing Disruptive Innovation Without Friction: Security for the Next-Generation Workforce
Tom Gillis, STBU VP and General Manager, Cisco

The emerging borderless network is leading us to a major productivity evolution where business advances at the speed of thought -- and the entire inner workings of a corporation can be accessed from the palm of your hand. To compete and survive in this new world, businesses must find ways to provide their workforce with "frictionless"—but secure—access to data. In this session, author and Internet security expert Tom Gillis provides an overview of the "disruptive innovation" in history and business that is shaping our modern information economy. He explains how smarter, flexible boundaries are needed to control and protect data, and shares Cisco's vision for securing the next-generation workforce.

12:15 pm - 1:30 pm   **Lunch and Discussion Tables**

Why Analysts Have Identified Virtual Directory as a Critical Element of the Emerging Identity Architecture

As more enterprises move to federation and the cloud, a single authoritative identity source no longer makes sense. Join this lunch discussion and find out why Gartner Group has identified Virtual Directory as a critical component to the emerging identity architecture. We'll discuss how the production of identities will be separated from the consumption of identities, and we'll explore how applications will externalize authorization to policy decision points that can use contextual authorization to request attributes in real time. *Hosted by Radiant Logic*

Practices for Testing, Measuring, and Communicating the Effectiveness of IT Security

Today's security professionals face many challenges, not the least of which is determining if the people, processes, and technologies that they've put in place to protect their company's information assets are actually effective. Despite the vast sea of security-related data most organizations already have at their fingertips, answers to simple questions like the following remain elusive:

-Are my most critical electronic data assets effectively protected from a breach?
-Is our security improving over time and providing ROI?

-Are we susceptible to the most recent emerging threats?

Participants in this discussion will have the opportunity to discuss and will be encouraged to share their own internal practices for testing, measuring, and communicating the effectiveness of IT security issues in their organizations. *Hosted by Core Security Technologies*

1:30 pm - 2:55 pm	**The Data Protection Standard: Business Track**	**The Data Protection Standard: Technology Track**
1:30 pm - 2:10 pm	**Breach Response**	**Securing Multiple Endpoints**
	Mark Connelly, Chief Information Security Officer, CISM, CGEIT, ITT	Dennis Devlin, Chief Information Security Officer, Brandeis University
		Moderator: Derek Slater, Editor in Chief, CSO magazine
		Jason Clark, Chief Security and Strategy Officer, Websense
	Even with the tightest security and most well-conceived policies, breaches happen, whether a company executive leaves a laptop in a cab or you discover stealth moves by a crime syndicate. Is your incident response plan ready? Hear from someone put to the test about their	Organizations' networks today reach across the globe and encompass many types of devices, from laptops to smartphones. Hear how leading

seminal moments, the proactive measures they've put in place, and what proved most valuable during their times responding to breach issues.

edge companies are securing all these endpoints and the lessons learned from quick rev mobile cycles, among other challenges.

| 2:15 pm - 2:55 pm | **Lock Down, Not Out with Encryption** | **Pick an Identity and Access Management Standard, Any Standard** |

Lock Down, Not Out with Encryption
David Escalante, Director of Computer Policy & Security, Information Technology Services, Boston College
Moderator: Bob Bragdon, Publisher, CSO magazine
Nick L. Kael, CISSP, Principal Security Strategist, Symantec

Pick an Identity and Access Management Standard, Any Standard
Andras Cser, Principal Analyst, Forrester Research

Encryption comes in many flavors and formats: from full-disk encryption to file encryption. Matching your encryption strategy to your business processes is the best way to ensure protection, access and performance

This discussion will examine some of the major standards in the identity world today -- like OpenID, SAML, OAuth, and the Trusted Platform Module -- and provide advice on understanding the relative pros and cons of each. Which are likely to emerge as the dominant standards, and why?

across the organization. This session will take you through various factors to consider in implementing encryption across the enterprise.

3:00 pm - 4:25 pm	**The Risk Management Standard: Business Track**	**The Risk Management Standard: Technology Track**
3:00 pm - 3:40 pm	**Proactive Protection Policies: Thwarting Social Engineering and Other Identity Challenges** Alan Lustiger, Director of Information Security, Gain Capital Holdings, Inc. Strong data protection strategies involve policy development and enforcement combined with smart technology deployment. Learn about	**Defining the Technical Governance and Risk Management Framework** Rajeev Yadav, Director, Information Security, Thomson Reuters The technical aspects of a governance and risk management framework are critical to overall risk management success. So how do you define the framework, sell it to the business, integrate it, and then get it work as you intended? Learn about the issues, challenges, and how do you deal

the latest, most effective practices for organizational education and follow-through to protect data from inadvertent or malicious data loss -- including training especially designed to spot social engineering.

with them from an expert on the subject.

| 3:45 pm - 4:25 pm | **Mitigating Risk by Re-evaluating 7 Key Areas of Your Business**
Nick Akerman, Partner, Dorsey & Whitney LLP | **Managing Virtualization's Security Risks**
JT Jacoby, Chief Security Officer, NYC Housing Authority |

CSOs and their teams can't make every information risk go away, but they can take some very simple steps to minimize it. How can you work most effectively with your legal, HR and compliance counterparts to reduce risk? What proactive steps can you take in advance to be prepared to respond to a data breach? In this session, get fresh tips on this and more from an information security legal expert.

Virtualizing and isolating servers by function (such as e-mail or web services) has security benefits, but there are other potential loopholes to virtualization. This session will help you examine those security risks, like system complexity, potential duplication of malicious code and artifacts left in memory, and determine how to best mitigate those risks.

4:25 pm   **Event Concludes**