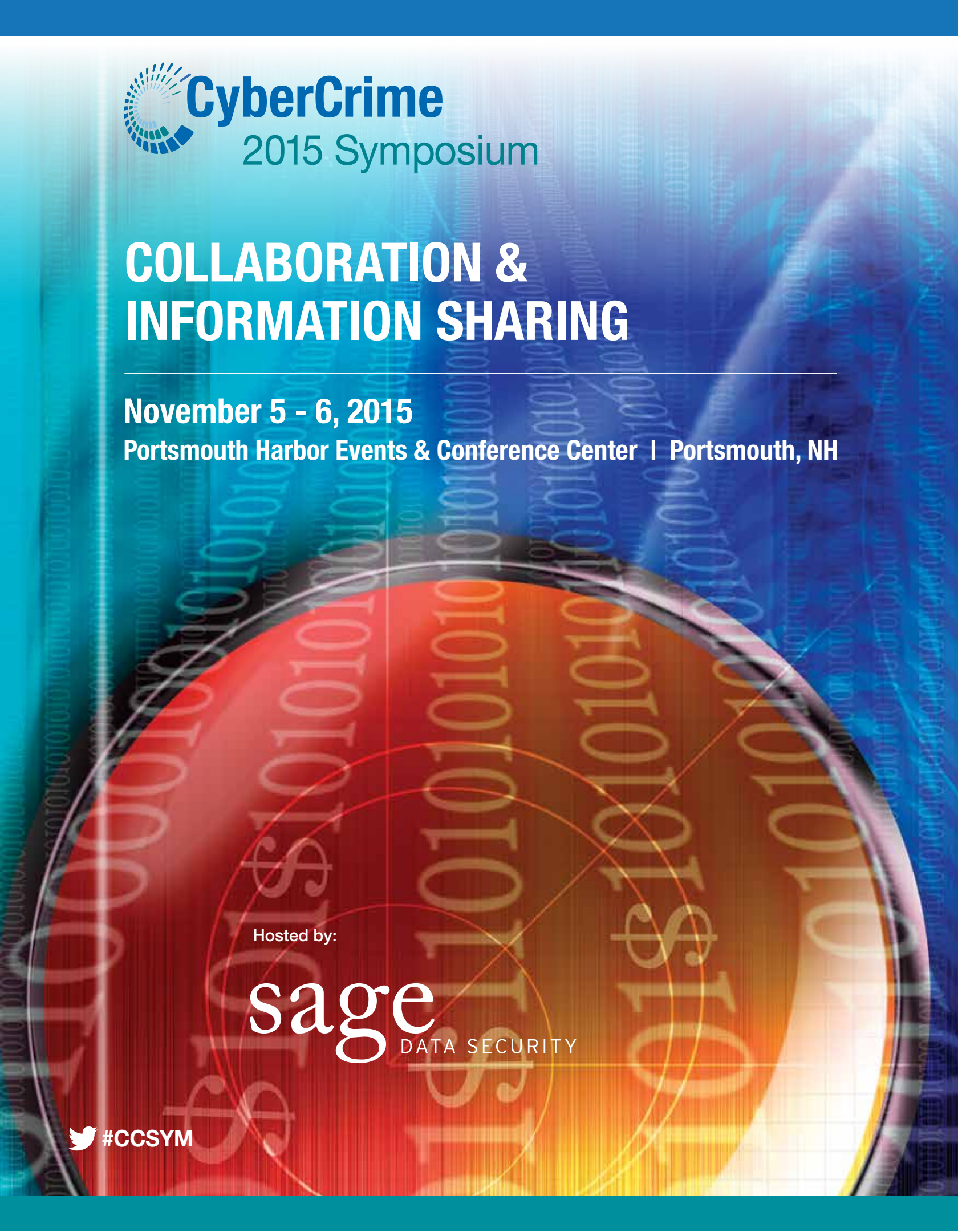
CyberCrime 2015 Symposium

COLLABORATION & INFORMATION SHARING

November 5 - 6, 2015

Portsmouth Harbor Events & Conference Center | Portsmouth, NH



Hosted by:

sage DATA SECURITY

#CCSYM

CyberCrime Symposium

2015 CYBERCRIME SYMPOSIUM AGENDA

Program is subject to change.

DAY ONE: Thursday, November 5, 2015

Registration: 11:15 a.m. – 11:45 a.m.

Welcome & Opening Remarks: 11:45 a.m. – 12:15 p.m.

Collaboration & Information Sharing

Sari Stern Greene, Sage Data Security Host Representative

We are all in this together. The need for cybersecurity collaboration and information sharing has never been greater. The challenge is how to balance common good partnerships with confidentiality and privacy requirements, free market competition and liability protection.

Sari Stern Greene, CRISC, CISM, CISSP-ISSMP is the founder of Sage Data Security and chair of the CyberCrime Symposium. She is the author of *Security Program and Policies: Principles and Practices*, as well as the recently released CISSP Complete Video Course. Sari advises Senior Management and Directors on information cybersecurity issues including strategic planning and incident management. T: @sari_greene

Lunch: 12:15 p.m.

Lunch Keynote: 12:15 p.m. – 1:15 p.m.

Stuxnet and Beyond: The Age of Digital Warfare

Kim Zetter, Author and Journalist

In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at a uranium enrichment plant in Iran were failing at an unprecedented rate. Five months later, a seemingly unrelated event occurred when researchers with a computer security firm in Belarus were called in to investigate why computers in Iran were crashing repeatedly. What they stumbled upon was the world's first digital weapon, Stuxnet. Kim Zetter will tell the story of Stuxnet's planning, execution, and discovery; why the attack was so unique, and the implications to the U.S. critical infrastructure.

Kim Zetter is an award-winning journalist who covers cybercrime, civil liberties, privacy, and security for Wired magazine. She is the author of *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Kim has covered hackers and computer security since 1999 and has broken numerous stories over the years about NSA surveillance, WikiLeaks and Bradley Manning (Chelsea Manning), and the hacker underground. T: @KimZetter

Afternoon Session I: 1:30 p.m. – 2:30 p.m.

IoT, When Things Crawl into Your Corporate Network

Uri Rivner, Head of Cyber Strategy at BioCatch and
Sam Curry, Chief Technology and Security Officer at Arbor Networks

IoT is coming to the corporate network. From worrying about PCs, servers, and printers, you'll begin to worry about THINGS: inter-connected, exponentially growing, access-hungry, and yours to control. In this session, we'll explore the IoT landscape, define what IoTs are, explore the risks of IoT security breaches, and see what we can do about them - if anything at all.

Uri Rivner has been fighting cybercrime for 12 years. Currently leading the cyber strategy for behavioral biometrics company BioCatch, Uri's prior role was Head of New Technologies, Identity Protection at RSA. Innovations that Uri spearheaded now stop billions of dollars in fraud each year and protect hundreds of millions of online banking and eCommerce users. T: @UriRivner

Sam Curry is the Chief Technology and Security Officer at Arbor Networks. Prior to joining Arbor Networks, Sam was SVP of Information Security and CISO at MicroStrategy. He has also served in significant roles at RSA, McAfee and Computer Associates. Sam is a frequent speaker and widely quoted subject matter expert. T: @SamJCurry

Afternoon Session II: 2:45 p.m. – 3:45 p.m.

Creating Honeypots for Tracking Criminals

Terrence Gareau, Chief Scientist at NEXUSGUARD

Digital innovation has created new attack surfaces for hackers to exploit. These same innovations and technological improvements have allowed researchers to create and deploy highly automated and scalable honeypots to lure and trap criminals. In this session, Terrence will describe the creation of a botnet used by NEXUSGUARD to track attacks and cyber-criminals to extract valuable data for defender intelligence.

As NEXUSGAURD's Chief Scientist, Terrence "Tuna" Gareau leads various teams in the development of security testing policies, network forensics strategies, and plans to protect client networks. Previously, he was Principal Research Scientist for A10 Networks, Inc. Terrence has more than 13 years of experience in IT security, including significant work with management of DDoS attacks. His knowledge has been shared with several high-level organizations, including IT security groups such as DEF CON and NoVa Hackers, and government agencies. T: @kingtuna

Afternoon Session III: 4:00 p.m. – 5:00 p.m.

Breaking In Bad (I'm The One Who Doesn't Knock)

Jayson E. Street, Social Engineer

Jayson does some weird social engineering engagements. In this presentation, Jayson will share his techniques including the roles he plays and the tactics that would have stopped him from being successful. He will demonstrate how EASY these attacks are and how every single attack has one common thread!

Jayson E. Street is an author of *Dissecting the Hack: The F0rb1dd3n Network* from Syngress and the creator of dissectingthehack.com. He has spoken at DEFCON, DerbyCon, UCON, and at several other 'CONs' and colleges on a variety of Information Security subjects. He is a highly carbonated speaker who has partaken of pizza from Beijing to Brazil. T: @jaysonstreet

Afternoon Session IV: 5:00 p.m. – 5:30 p.m.

A Chat with Secret Service Agent Matt O'Neill

Matthew O'Neill, Special Agent, U.S. Secret Service

New England businesses experience their share of cybercrime. SA O'Neill will brief us on recent cases and investigations. Then, by popular demand, we'll open up the session for questions from the audience.

Matthew O'Neill won the Department of Homeland Security Silver Medal in 2014 and the USSS Special Agent of Year Award in 2013 for his efforts in investigating complex transnational cyber-crime investigations including network intrusions, point of sale terminal compromises, bulk online sale of stolen personally identifiable information, money laundering, bank fraud, counterfeit currency cases, wire fraud, and insurance fraud cases. SA O'Neill joined the US Secret Service in December 1998. Since 2007, he has been assigned to the Manchester, New Hampshire, office.

Cocktails: 5:30 p.m. – 6:15 p.m.

Dinner Buffet: 6:15 p.m.

Dinner Keynote: 7:00 p.m. – 8:00 p.m.

Securing Boomers, Gen Xers, and Millennials: OMG We are So Different!

Todd Fitzgerald, Global Director of Information Security at Grant Thornton International, Ltd.

You may have noticed lately that the workforce is changing. We now have 3 generations working side by side, with a fourth about to join us. Why are we so different? Why do we approach work differently and have different values? What are the implications for information security? This interactive session explores differences between the generations in a fun and informative way!

Todd Fitzgerald is the Global Director of Information Security for Grant Thornton International, Ltd. and a Ponemon Institute Distinguished Fellow. He is the author of *Information Security Governance Simplified: From the Boardroom to the Keyboard*, and co-author of the ISC2 Book, *CISO Leadership: Essential Principles for Success*. Prior leadership positions include ManpowerGroup, WellPoint (National Government Services), Zeneca, Syngenta, IMS Health, American Airlines and Blue Cross Blue Shield. T: @securityfitz

Share your CyberCrime insights on twitter using #CCSYM

Follow us @cybercrimesym

DAY TWO: Friday, November 6, 2015

Breakfast Buffet: 7:30 a.m.

Breakfast Keynote: 8:00 a.m. – 9:00 a.m.

The Long Road to a Secure Web

Andy Ellis, Chief Security Officer at Akamai

In a world of pervasive monitoring, content injection, and other vexatious adversaries, getting to a secure web experience requires more than just a TLS certificate. Let's look under the covers of TLS web implementations, and understand the hazards we all face, and the steps forward towards a safer future.

Andy Ellis is Akamai's CSO, responsible for overseeing the security architecture and compliance of the company's massive, globally distributed network. He is the designer and patent holder of Akamai's SSL acceleration network, as well as several of the critical technologies underpinning the company's Kona Security Solutions. Andy is a graduate of MIT and a former US Air Force Officer, the recipient of the CSO Magazine Compass Award, the Air Force Commendation Medal, The Wine Spectator's Award of Excellence, and the Spirit of Disneyland Award. T: @csoandy

Morning Session I: 9:15 a.m. – 10:15 a.m.

The Evolving NIST Cyber Framework

Adam Sedgewick, Sr. Info Technology Policy Advisor at NIST

In February 2014, NIST released the NIST Cybersecurity Framework for voluntary use in all critical infrastructure sectors, including financial services, government and healthcare. In this session, Adam will review the key elements of the Cybersecurity Framework, share adoption and implementation feedback, and discuss how the Cybersecurity Framework will evolve in the coming months and years.

Adam Sedgewick is the Senior Information Technology Policy Advisor at the National Institute of Standards and Technology (NIST). He was one of the key members of the NIST team involved with the creation of the Cybersecurity Framework and continues to spearhead efforts on behalf of the Framework's development and long-term goals. In 2008 and 2013, Adam received the Fed 100 Award for his contributions to the federal information technology community.

Morning Session II: 10:30 a.m. – 11:30 a.m.

FS-ISAC Threat Intelligence Ecosystem

Rick Lacafta, Director of Insurance Services at FS-ISAC

FS-ISAC threat intelligence is being used nationwide by financial institutions. Rick will detail the ISAC intelligence sharing ecosystem, and how intelligence is shared between members, government partnerships, and additional intelligence sources. The session will include a discussion on the need for intelligence automation and the strategy to address that need.

Rick Lacafta has over 40 years of experience in information technology, information security and legal compliance management with Travelers Insurance, Citigroup, Primerica and CitiFinancial and most recently, as the Director of Insurance Services at the FS-ISAC where he manages the Insurance Risk Council, Community Institution Council, and Compliance and Audit Council.

Morning Session III: 11:45 a.m. – 12:15 p.m.

.Bank Update - What You Need to Know

Doug Johnson, SVP and Chief Advisor, Payments and Cybersecurity Policy at American Bankers Association

The new .BANK top level domain has received over 6,000 registrations since going live on June 23, 2015. Conceived by our industry as a trusted, verified and more secure location online for banks, their customers and their stakeholders, this session will discuss the challenges and opportunities bankers are currently addressing as they implement their domains.

As the ABA's Senior Vice President, Payments and Cybersecurity Policy, Doug Johnson is involved in a variety of public policy and compliance issues. He currently leads the Association's enterprise risk, physical and cyber security efforts, in addition to business continuity and resiliency policy and fraud deterrence efforts. Doug serves as Vice Chairman of the Financial Services Sector Coordinating Council and is a Board member of the FS-ISAC.

Lunch Buffet: 12:15 p.m.

Lunch Keynote: 12:45 p.m. – 1:45 p.m.

Engineering Privacy: Why Security Isn't Enough

J. Trevor Hughes, President and CEO of the International Association of Privacy Professionals

If we're going to take hacking seriously, what needs to happen are far more sophisticated data-handling techniques behind the walls we erect. This is where privacy professionals can step into the breach (pun intended), working hand in hand with IT and cybersecurity professionals to identify and inventory data, make sure it's all useful and necessary, and then most importantly, make sure that data is virtually useless to the outside world should the hackers get in.

J. Trevor Hughes is the President and CEO of the International Association of Privacy Professionals (IAPP), the world's largest association of privacy professionals. Trevor is an experienced attorney in privacy, technology and marketing law. He has provided testimony on privacy issues before several committees within the U.S. Congress, British Parliament and EU Parliament. He is an adjunct professor of law at the University of Maine School of Law and frequently speaks about privacy issues at conferences around the world. T: @jtrevorhughes

Afternoon Session I: 2:00 p.m. – 3:00 p.m.

The Internet is a Battlefield

Shane Harris, Author and Journalist

Espionage and warfare are being conducted via computer connections, profoundly changing the nature of intelligence and warfare in the 21st Century. In this session, Shane explores the new dimensions of the "fifth domain of warfare," and will explain how cyber security became a top national security concern for the U.S. government. He'll also examine how recent high-profile breaches at major U.S. companies – including Sony and Home Depot – as well as the hack of the Office of Personnel Management, are changing the nation's response to cyber threats.

Shane Harris is the author of *@War: the Risk of the Military-Internet Complex* (2014) and *The Watchers* (2010). He is currently a senior correspondent at The Daily Beast, where he covers national security, intelligence, and cyber security. He is also an ASU Future of War Fellow at New America. His work has appeared in The New York Times, The Wall Street Journal, Slate, TheAtlantic.com, National Journal, The Washington Post, The Bulletin of the Atomic Scientists, and the U.S. Naval Institute's Proceedings.
T: @shaneharris

Afternoon Session II: 3:00 p.m. – 3:30 p.m.

Using Musical Principles to Contextualize Security: A Jam Session!

David Scott, Software and Data Management Professional

Can Beethoven's Fifth Symphony predict future cyber events? Does jazz music impact our choice of security tools? Both sound and security events have timbre, style, structure, volume, rhythm, and history. We explore the ways musical concepts such as motifs, chord structures, and improvisation enhance our understanding of security and help us predict future cyber events. This is no mere lecture - join the JAM and EXPERIENCE it!

David Scott is a software and data management professional with over 20 years of creative and operational success in all aspects of IT product and services delivery. Beyond the IT world, David is known as a vocalist and choral/orchestral conductor.
T: @cannotbesilent