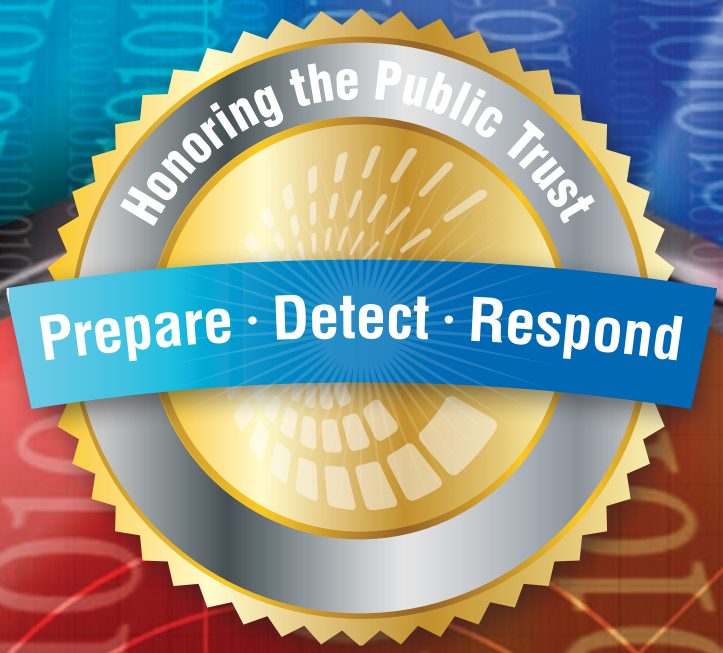
CyberCrime 2013 Symposium

Prepare, Detect & Respond: Honoring The Public Trust

November 14–15, 2013

Portsmouth Harbor Events & Conference Center | Portsmouth, NH



Hosted by:

sage DATA SECURITY

CyberCrime 2013 Symposium

DAY ONE AGENDA: Thursday November 14, 2013

Program is subject to change.

Registration: 11:30 a.m. – 12:00 p.m.

Welcome and Opening Remarks: 12:00 p.m. – 12:15 p.m.

Working Together to Honor the Public Trust

Speaker: Sari Stern Greene, *Sage Data Security Host Representative*

CyberCrime is escalating at an alarming rate. The challenge to each of us is how to protect the information and systems with which we have been entrusted. We need to work together as individuals, companies and communities; to exchange ideas and to share our knowledge, enhancing our ability to protect and defend our customers, our organizations and our community against cybercriminals.

Sari Stern Greene, CRISC, CISM, CISSP is the founder of Sage Data Security. She is a recognized leader in the field of information security, and the author of *Security Policies and Procedures: Principles and Practices*, used in undergraduate and graduate programs nationwide. Sari advises Senior Management and directors on information security issues and strategic planning. She is Chair of the CyberCrime Symposium, a member of several security working groups, a frequent lecturer at colleges and universities and a supporter of regional ISACA and ISC2 organizations.

Lunch Keynote: 12:15 p.m. – 1:30 p.m.

When Cybercrime Gets Personal

Speaker: Brian Krebs, *Editor KrebsonSecurity.com*

Security pros like to remind us that most cybercrime isn't personal. Rather, it's more about probabilities: if your precious data is left unprotected, it can (and eventually will) be extracted and monetized. Drawing on his experience as the target of an arsenal of kinetic and cyber attacks, veteran cybersecurity journalist Brian Krebs will discuss preparing for the inevitable and how to take back control over our personal and financial data.

Brian Krebs is the editor of *Krebsonsecurity.com*, a daily blog dedicated to in-depth cyber security news and investigation. For the third year running, KrebsonSecurity.com was voted the blog that best represents the security industry by judges at the 2013 RSA Conference. He was also presented with the "Security Bloggers Hall of Fame" award, alongside noted security expert Bruce Schneier. Krebs worked as a reporter for *The Washington Post* from 1995 to 2009, where he covered internet security, cybercrime and privacy issues for the newspaper and the website. His stories and investigations also have appeared in *Popular Mechanics*, *MIT Technology Review*, *CSOonline* and *Wired.com*.

Afternoon Session I: 1:45 p.m. – 2:45 p.m.

Speed and Sophistication: Takeaways from the 2013 Verizon Data Breach Investigations

Speaker: Wade Baker, *Verizon Managing Principal of Research and Intelligence*

Sophistication, along with speed, was one of the two themes that stood out in the 2013 *Data Breach Investigations* report. Attackers are smart. When it comes to protecting systems and data, there's no room for complacency. Your security measures are probably a lot more sophisticated than they were a few years ago, but so are the attackers. From disaffected activists to state-affiliated actors, malware to denial of service, the threats are numerous and varied. Now in its sixth year of publication, the 2013 data breach report includes 621 confirmed data breaches as well as more than 47,000 reported security incidents. Verizon is joined by 18 worldwide organizations that contributed data and analysis to this year's report. Understanding the sophistication of the attackers and their tactics will help you to adopt a smarter approach to protecting your business.

Wade Baker is the Managing Principal of Research and Intelligence with Verizon's RISK Team. He is the creator and lead author of the Verizon's Data Breach Investigations Report and the Payment Card Industry Compliance Report series. A researcher at heart, Baker's work on various topics has been published in a number of academic journals, professional magazines, industry reports, and books. He had the privilege of consulting with the President's Information Technology Advisory Council, and his research was featured in the 2005 Report, "Cyber Security: A Crisis of Prioritization." His PhD dissertation explores the use of decision support systems to improve information security operations and management decision-making.

Afternoon Session II: 3:00 p.m. – 4:00 p.m.

Everything You Need To Know About A DDoS Attack

Speaker: Andrew Sullivan, *Internet Engineering Task Force (IETF) & Director of DNS Engineering at Dyn*

In the last year, DDoS attacks have been a recurring topic, and the way things are going, they will continue to be a major issue in the years ahead. Big companies and brands have been victims of attacks that continue to grow in size and complexity but DDoS attacks can happen to companies of any size. What is a DDoS attack and how do you know if you're the target of one? What do you do if you are a victim? How could a DDoS attack affect your business? This session will answer all of these questions, and tell you what's needed to create a defense plan and respond to and mitigate DDoS attacks.

Andrew Sullivan is a member of the Internet Architecture Board (IAB), the Internet Engineering Task Force (IETF) and is Director of DNS Engineering at Dyn. Previously, he worked on future innovations for Dyn as Director of Labs. Mr. Sullivan has long been a leading voice in the DNS and Internet community and previously worked as the Director of Name Services at Afilias and as an Internet Scientist at Shinkuro, Inc.

Afternoon Session III: 4:15 p.m. – 5:15 p.m.

Cybercrime and the Law: Challenges, Issues, and Outcomes

Speaker: **Susan Brenner,** *Author & NCR Distinguished Professor of Law and Technology*

The exponential increase in cybercrime in the past decade has raised new issues and challenges for both national and international law enforcement. Illuminating legal issues unique to investigations in a digital environment, Brenner examines both national law enforcement agencies and transnational crime, and shows how cyberspace erodes the functional and empirical differences that have long distinguished crime from terrorism and both from warfare.

Susan Brenner specializes in two distinct areas of law: grand jury practice and cyberconflict, i.e., cybercrime, cyberterrorism and cyberwarfare. A member of the American Academy of Forensic Sciences, Professor Brenner has spoken at numerous events, including two Interpol Cybercrime Conferences, the Middle East IT Security Conference, the American Bar Association's National Cybercrime Conference and the Yale Law School Conference on Cybercrime. She spoke on cyberthreats and the nation-state at the Department of Homeland Security's Global Cyber Security Conference and participated in a panel discussion of national security threats in cyberspace sponsored by the American Bar Association's Standing Committee on Law and National Security.

Cocktail Hour: 5:15 p.m. – 6:00 p.m.

Dinner: 6:00 p.m. – 6:30 p.m.

Dinner Keynote: 6:30 p.m. – 8:00 p.m.

Speaker: **Jeremy Zerechak,** *Director, "Code 2600"*

Director Jeremy Zerechak will introduce the film and moderate a post-screening Q & A session; every attendee will receive a DVD of the film. Both enlightening and disturbing, "CODE 2600" documents the rise of the Information Technology Age as told through the events and people who helped build and manipulate it. The film explores how we struggle to comprehend the socio-technical fallout caused by data collection and social networks, while our modern culture is caught in an undercurrent of cyber-attacks, identity theft and privacy invasion.

Jeremy Zerechak is an accomplished documentarian and film technician who has produced and directed two award winning feature-length documentaries: "Land of Confusion" chronicles his Army unit's mission in Iraq and the operations of the Iraq Survey Group; and "CODE 2600," his documentary about the evolution of the Information Technology Age and computer hacker culture. Mr. Zerechak is also a decorated Iraq War veteran and an advocate for veteran rights. He currently teaches and studies film at the Ohio University School of Film. He has received the Special Jury Awards at both the Florida Film Festival and Atlanta Film Festival for "Land of Confusion"; and the Grand Jury Award for Best Documentary 2013, Atlanta Film Festival, for "CODE 2600."

DAY TWO AGENDA: Friday November 15, 2013

Breakfast: 7:30 a.m. – 8:15 a.m.

Breakfast Keynote: 8:15 a.m. – 9:15 a.m.

The Future of Payments: Secure Mobile Payment Architecture

Speaker: **Neil Bergman,** *Senior Security Consultant, Cigital*

Some analysts are predicting that close to $100 billion will be spent via mobile payment systems by 2017. Mobile payments have some clear advantages over magnetic stripe cards, but the mobile payment systems currently in use have different attack surfaces that can be exploited in both traditional and novel ways. In this talk, we will explore the attack surfaces of mobile payment architectures, including NFC-based wallets. We'll dive into the design of the mobile payment clients and the back-end applications, review the known attacks against these systems, and explore countermeasures that system architects, developers and security practitioners can adopt to harden their systems.

Neil Bergman is a senior security consultant at Cigital and co-author of *Hacking Exposed Mobile Security Secrets & Solutions*. He has led and conducted penetration testing, code review, and architecture risk analysis of critical applications for industry-leading financial and software companies. Mr. Bergman has conducted security assessments on a multitude of mobile platforms as well as against web services, web applications, and thick clients.

Morning Session I: 9:30 a.m. – 10:45 a.m.

Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects

Speaker: **Brett Shavers,** *Noted Author and Forensic Investigator*

How can an investigator affirmatively place a suspect at the keyboard? This presentation gives investigators and analysts guidance on workflow processes, digital forensics capabilities, traditional investigative methods, information management and analysis, and case presentation tips in order for you to put a cybercrime case together, from inception to prosecution.

Brett Shavers is the author of *Placing the Suspect Behind the Keyboard*, which integrates traditional investigative methods with high-tech forensic analysis to build a solid criminal or civil case, and *The Practitioner's Guide to X-Ways Forensics*. Currently serving as President of the Computer Technology Investigators Network (CTIN), Mr. Shavers began his career as a digital forensics investigator in law enforcement and was trained by the Federal Law Enforcement Training Center, the U.S. Department of Homeland Security, the National White Collar Crime Center, AccessData, X-Ways Forensics, and other forensic software manufacturers. He now owns his own electronic discovery company. Mr. Shavers has testified as a computer forensics expert, has been court appointed as a Special Master, and has given multiple depositions in civil and criminal matters ranging from internal corporate matters to class action litigation.

Morning Session II: 11:00 a.m. – 12:30 p.m.

Lessons Learned from the Boston Regional Catastrophic Cyber Disruption Planning Project

Speaker: Adam Wehrenberg and **Kevin O'Shea,** *Project Directors, New England Regional Catastrophic Planning Initiative, Boston Office of Emergency Management*

As recent events in Boston proved, disaster response planning and exercising played a significant role in saving lives and ensuring a prompt recovery following the terrorist attacks in April. Adam Wehrenberg and Kevin O'Shea will share their work on the Boston-based project to develop a regionalized response to a large-scale cyber disruption. The lessons learned are applicable to any organization reliant on interconnected and complex systems and public infrastructure.

Adam Wehrenberg is responsible for the oversight of catastrophic planning activities in the New England Regional Catastrophic Preparedness Initiative (NERCPI), which includes Massachusetts, New Hampshire and Rhode Island, as well as the Boston and Providence Urban Areas Security Initiative (UASI) regions. Prior to his current role, he served the Massachusetts Office Of Emergency Management (OEM) and as Public Safety Manager for Emergency Preparedness for the Massachusetts Convention Center Authority (MCCA).

Kevin O'Shea has years of experience in technical project management for cybersecurity, emergency response, and infrastructure resiliency. His efforts to regionalize the State and local response to a catastrophic loss of IT and communications for the NERCPI culminated in the development of a Cyber Disruption Response Annex.

Lunch: 12:15 p.m. – 12:45 p.m.

Lunch Keynote: 12:45 p.m. – 1:45 p.m.

What's Going On in Washington?

Speaker: Doug Johnson, *Vice President and Senior Advisor, Risk Management Policy, American Bankers Association*

"Our country's reliance on cyber systems to run everything from power plants to pipelines to hospitals and highways has increased dramatically, and our infrastructure is more physically and digitally interconnected than ever. Yet for all the advantages interconnectivity offers, critical infrastructure is also increasingly vulnerable to attack from an array of cyber threats." – *DHS Fact sheet, February 13, 2013*

In February 2013, the White House issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity. Citing repeated cyber-intrusions into critical infrastructure (which includes the financial and healthcare sectors), the order calls for voluntary, collaborative efforts involving both federal agencies and privately owned companies. The Executive Order also directs the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework to reduce cyber risks to critical infrastructure. This session will focus on the potential impact of the Cybersecurity Framework and the success of current public/private partnership programs.

Doug Johnson is the American Bankers Association's Vice President and Senior Advisor, Risk Management Policy, where he currently leads the association's enterprise risk, physical and cyber security, business continuity and resiliency policy and fraud deterrence efforts. Mr. Johnson serves as Vice Chairman of the Financial Services Sector Coordinating Council, which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues, and is a board member of the Financial Services Information Sharing and Analysis Center.

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

Recognizing National Cyber Security Awareness Month (#ncsam)

Speaker: Michael Kaiser, *Executive Director of the National Cyber Security Alliance*

National Cyber Security Awareness Month (NCSAM) is a national public awareness campaign encouraging everyone to protect their computers and our nation's critical cyber-infrastructure. This October marked the 10th anniversary of National Cyber Security Awareness Month; the 2013 theme was "Our Shared Responsibility." Our closing session will discuss how individuals, organizations, and communities across the nation promote NCSAM using social media, education and more. Learn how your organization can become a NCSAM Champion – search for #ncsam.

Michael Kaiser serves as Executive Director of the National Cyber Security Alliance (NCSA), which builds public-private partnerships that address cyber security issues for home users, education, and small business. Mr. Kaiser serves on the Department of Commerce NTIA Online Safety and Technology Working Group.