



CyberCrime

2011 Symposium

Security in the Age of WikiLeaks – Cybercrime, Espionage & Hacktivism

November 3-4, 2011


Sheraton Portsmouth Harborside Hotel | Portsmouth, NH

Hosted by:

sage
DATA SECURITY

NOVEMBER 3, 2011 • DAY ONE: Data Insecurity


 **Registration**
11:00 a.m. – 12:00 p.m.

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

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

2011 has been an unprecedented year of data compromise, exposure and harm. We've witnessed the unauthorized taking of secret diplomatic cables by Private Manning and subsequent publication on WikiLeaks; the hacktivism of "Anonymous" and "LulzSec"; the stealing of information from Sony, Epsilon, RSA, Fox, NASA and dozens of other major corporations, hospitals and government agencies; and the theft of Internet Banking credentials from small business and municipalities nationwide. A combination of smart cybercriminals, sophisticated malware, lax security policies and a "cool" factor associated with hacking has made 2011 an exceptional year. To combat these growing threats, new laws and regulations are being introduced at every level of government. Best case scenario: your organization has implemented safeguards to mitigate the risk and meet compliance requirements. Worst case scenario: you experience the triple whammy of cybercrime, enforcement action and litigation! Which will it be?


Sari Stern Greene is a recognized leader in the field of information security, and the author of *Security Policies and Procedures: Principles and Practices*, which is being used in undergraduate and graduate programs nationwide. Greene is an active member of several national security advisory groups, a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Manager (CISM) and is certified by the National Security Agency to conduct NSA-IAM assessments for federal government agencies and contractors.

 **Lunch Keynote**
12:15 p.m. – 1:30 p.m.

WikiLeaks – Is Any Secret Safe?

In June 2010, Kevin Poulsen and a co-writer broke the news that the government had secretly arrested a young Army intelligence analyst on suspicion of leaking hundreds of thousands of classified documents to WikiLeaks. Poulsen subsequently published the logs of Bradley Manning's incriminating chats with Adrian Lamo. In some 70+ stories, Poulsen and staff have diligently charted WikiLeaks' successes, and its setbacks. Poulsen will share his knowledge of the organization, the Manning incident, the publication of classified documents and how WikiLeaks has impacted the world.

Speaker: Kevin Poulsen, Senior Editor, *Wired.com* and author of *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*, is an award-winning investigative journalist (and reformed hacker), who oversees news and feature reporting at *Wired.com*. For five years he served as editor of the *Threat Level* blog, which under his tenure won the 2008 Knight-Batten Award for Innovation in Journalism, the 2010 MIN award for best blog and both Webby and People's Voice awards in 2011.


 **Afternoon Session I**
1:45 p.m. – 3:00 p.m.

50 Days of Mayhem: What We Can (and Should) Learn from LulzSec

"For the past 50 days we've been disrupting and exposing corporations, governments, often the general population itself, and quite possibly everything in between, just because we could. All to selflessly entertain others – vanity, fame, recognition, all of these things are shadowed by our desire for that which we all love. The raw, uninterrupted, chaotic thrill of entertainment and anarchy." (LulzSec Published Statement, 6/25/11)

LulzSec didn't invent hacktivism, but its small crew of hackers whose motto is "Laughing at your security since 2011!" merrily sailed the cyber-seas for 50 days of mayhem that became perhaps the biggest tech story of the first half of 2011. LulzSec caused (and is still causing) sleepless nights for security professionals around the world. Jerry Gamblin will discuss what they did, how they did it, and how we should have been able to stop them.

Speaker: Jerry W. Gamblin, Security Specialist, Missouri House of Representatives. Gamblin has been the Network Security Specialist for the Missouri House of Representatives since 2005. He manages the Missouri House of Representatives security program and speaks regularly to security groups around the country about network security and security awareness issues.

 **Afternoon Session II**
3:15 p.m. – 4:30 p.m.

The Malware Behind the RSA Breach and other Advanced Persistent Threats

Although the definition of APT can vary, experts agree that "advanced persistent threats" are primarily used for cyber-espionage activity targeted at government or industry. While working on a project to classify 60 different families of custom malware that have been used in APT/cyber-espionage attacks, researchers at Dell SecureWorks concluded that the breach of RSA last spring – in which sensitive information related to RSA SecurID tokens was stolen – can be traced back to an attack originating in China. Joe Stewart, Director of Malware Research for Dell SecureWorks, announced their findings at the August 2011 Black Hat Conference. Based upon the findings, Dell SecureWorks developed and publicly distributed Snort-based signatures to detect this particular APT. Stewart will update us on their research and conclusions.

Speaker: Joe Stewart is Director of Malware Research for Dell SecureWorks' Counter Threat Unit (CTU). An expert on Internet threats, Stewart was the first to discover the interworkings of the Clampi Trojan, which has stolen tremendous amounts of data, including banking credentials, from infected corporate and home computers. He is a frequent commentator on security issues for the *Wall Street Journal*, *The New York Times*, *Washington Post*, and *USA Today*, and has presented his security research at many conferences worldwide.

Afternoon Session III 4:45 p.m. – 5:45 p.m.

Respond and Defeat – 2011 Secret Service Cyber Intelligence Update

The Secret Service established the Cyber Intelligence Section (CIS) within its Criminal Investigative Division to combat the rise in cybercrime targeting the nation's financial payment systems and critical infrastructures. Through Secret Service cybercrime investigations, open source Internet content and a variety of information obtained through financial and private industry partnerships, the CIS serves a critical investigative support function for the collection of data related to hacking, identity theft, credit card fraud, bank fraud and computer related crimes. Special Agent Erik Rasmussen will share with us how the CIS successfully investigates, prosecutes and works to dismantle international and domestic criminal organizations.

Speaker: Secret Service Special Agent Erik Rasmussen is currently assigned to the Criminal Investigative Division, Cyber Intelligence Section. Prior to this assignment, Special Agent Rasmussen worked on the Electronic Crimes Task Force for the Los Angeles Field Office and Seattle Field Office.

Cocktails and Networking with Colleagues and Speakers 5:45 p.m. – 6:30 p.m.

Dinner and Dinner Keynote 6:30 p.m. – 8:00 p.m.

Krebs on Security: ZeuS, Thieves and Money Mules

Cybercriminals have continued their assault on businesses, municipalities, school districts and non-profits. Investigative reporter and journalist Brian Krebs has been tracking their activity and has broken more than 100+ stories exposing the exploits of Eastern European organized crime groups that are stealing tens of millions of dollars from companies through online bank account hijacking, fake anti-virus scams, ATM heists, sophisticated malicious software, and a seemingly limitless supply of accomplices here in the United States and in Europe. Krebs will share an insider's observation of organized cybercrime gangs that are often tolerated or even sponsored by their host countries and sometimes at war with each other!

Speaker: Brian Krebs is the editor of Krebsonsecurity.com, a daily blog dedicated to in-depth cyber security news and investigation. Krebs worked as a reporter for *The Washington Post* from 1995 to 2009, authoring more than 1,300 blog posts for the *Security Fix* blog, as well as hundreds of stories for washingtonpost.com and *The Washington Post* newspaper, including eight front-page stories in a *Post Magazine* cover piece on botnet operators. In 2010, Krebsonsecurity.com was named the best non-technical security blog at the RSA Security Conference.

After Dinner Panel Moderated by Brian Krebs 8:00 p.m. – 9:00 p.m.

OMG – I've been attacked!

You've been unexpectedly plunged into the abyss of a cybercriminal attack. What does it take to survive? Our after dinner panel will share with you their first-hand experience of responding to and dealing with the effects of cybercrime. The panel will be moderated by Brian Krebs, who will share his experience of being attacked. Panelist will represent a spectrum of organizations including a financial institution, a hospital, and a government agency.

NOVEMBER 4, 2011 • DAY TWO: Incident Response & Management

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

“Learn from the Mistakes of Others: Be Better Prepared to Combat Security Risks to Your Organization” ~ Insights from the 2011 Verizon Data Breach Investigations Report

The Data Breach Investigations Report series now spans seven years and more than 1,700 breaches involving more than 900 million compromised records. It offers an unparalleled view into cybercrime around the world. This year's report includes data from the United States Secret Service and the Dutch National High Tech Crime Unit, and covers 761 data breaches involving nearly 4 million compromised records. Lead researcher Bryan Sartin will identify common trends, share insights and offer recommendations on how businesses can protect themselves from data breaches.

Speaker: Bryan Sartin is Director of Investigative Response at Verizon. As a senior forensic examiner, Sartin has taken the lead in many high-profile data compromise investigations around the world. Additionally, he is well-versed in both criminal and civil computer forensic procedures and is a certified expert witness.

Morning Session I 9:00 a.m. – 11:30 a.m.

What You Need to Know Before It Happens to You

The best defense is to be prepared. For this session, we have brought together a team of forensic, legal and industry experts to discuss what you need to know to minimize the impact of a malicious external attack, an insider threat, a vendor compromise or an accidental exposure.

- **Forensic Fundamentals** – Benjamin Greenfield, Security Engineer, Google (formally of Sage)
- **46 States and Counting: State & Federal Notification Requirements** – Peter Guffin, Attorney, Pierce Atwood
- **Public Relations Rapid Response** – Ross Levanto, Schwartz MSL

Speakers: Benjamin Greenfield, CISSP, is a Security Engineer at Google, Inc. His focus at Google is on detecting and preventing intrusions. Greenfield is a recent recipient of the SANS Digital Forensics Challenge coin. Prior to joining Google, he was a Senior Security Analyst for Sage Data Security.

Attorney Peter Guffin is the leader of Pierce Atwood's Privacy and Data Security Practice Group, a member of its Intellectual Property and Technology Practice Group, and Adjunct professor at the University of Maine School of Law. Guffin represents businesses in a wide range of industries, including information technology, energy, financial services, insurance and health care.

Ross Levanto is Vice President at Schwartz MSL, headquartered in Boston with offices in London, San Francisco and Stockholm. In 1996, he worked in Vice President Al Gore's communications office in Washington, D.C., where he performed background research for the Clinton administration's export encryption policies. Levanto also served as vice president, press and public affairs for the New England Business and Technology Association, which later merged with the Massachusetts Software Council.

Security in the Age of WikiLeaks – Cybercrime, Espionage & Hacktivism

November 3-4, 2011

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

Incident Response Exercise

Are you prepared to respond to an attack? This audience participation team simulation will challenge your plans, resources and assumptions with the objective of strengthening your organization's preparedness.

Lunch and Session III 12:30 p.m. – 2:00 p.m.

Cyber Insurance: Will You Be Covered if Your Company Suffers a Cyber Event?

The price tag on corporate data breaches is soaring. Does Cyber Risk Insurance make sense for your organization? Cyber Insurance policies generally cover third-party liability – e.g. suits filed by customers whose accounts have been hacked; direct costs – e.g. notification letters sent to affected customers; and, increasingly, fines and penalties associated with data breaches. This session will focus on what policy holders should be looking for in Cyber and Data Security Coverage and how to avoid potential pitfalls.

Speaker: Attorney Scott Godes is counsel in the Dickstein Shapiro Cyber Insurance Practice Group.

Godes focuses on representing corporate policyholders in insurance coverage disputes. He is a seasoned litigator who has extensive experience in trying complex insurance coverage disputes, including class actions, in state, federal, bankruptcy, and appellate courts, as well as in commercial arbitrations.

Recent publications include:

- "Insurance Coverage for Denial-of-Service Attacks," *Insurance Law Center Blog* (May 17, 2011)
- "Computer and Funds Transfer Fraud Endorsements Issues," *e-Commerce Law & Strategy* (January 2011)
- "Insurance Coverage for Cyberattacks and Denial-of-Service Incidents," *Agentsofamerica.org* (October 6, 2010)

Closing Session 2:00 p.m. – 3:00 p.m.

Making the Internet a Safer Place for our Children and our Community

Cyberbullying is a particularly brutal form of cybercrime. Cyberbullying is generally defined as the persistent and intentional use of electronic communication to harass, threaten, intimidate or otherwise mistreat, typically between or among youth. Approximately 20% of young people report experiencing cyberbullying in their lifetimes. Our closing session will focus on what each and every one of us can do to combat cyberbullying and make the Internet a safer place for our children and our communities.

Presented by A World of Difference® Institute. As a leading provider of anti-bias training and resources, the Institute offers innovative programming to help schools develop a comprehensive approach to prevent and intervene against cyberbullying as part of a broader strategy to create safe schools for all students.

Closing Remarks – Sari Greene 3:00 p.m. – 3:15 p.m.

sage DATA SECURITY

Protecting Information Assets. | Ensuring Regulatory Compliance. | Fighting Cybercrime.

Founded in 2002, **Sage** serves as a strategic security partner for financial institutions, healthcare providers, government agencies and businesses nationwide. Sage offers an award-winning portfolio of Advisory, Assessment and Incident Detection & Response services designed to protect information assets and ensure regulatory compliance.

For more information, visit www.sagedatasecurity.com and www.ndiscovery.com