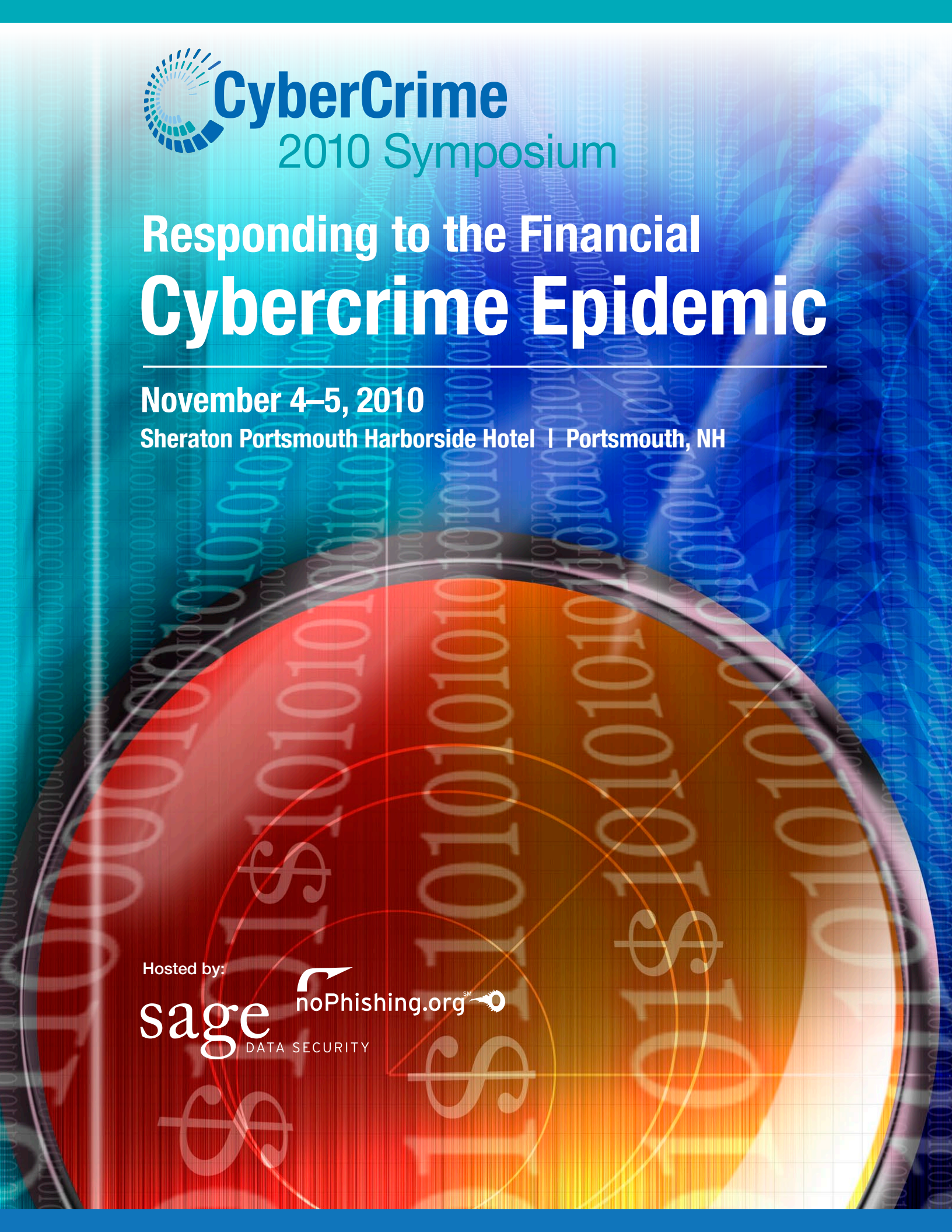
CyberCrime 2010 Symposium

Responding to the Financial Cybercrime Epidemic

November 4–5, 2010

Sheraton Portsmouth Harborside Hotel | Portsmouth, NH



Hosted by:

sage DATA SECURITY

noPhishing.org℠

CyberCrime 2010 Symposium

NOVEMBER 4, 2010 • DAY ONE

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, Managing Director MEAPC and President Sage Data Security

Lunch Keynote
12:15 p.m. – 1:15 p.m.

The Hunt for the New Crime Lords Who are Bringing down the Internet
Who is behind the meteoric rise in financially motivated cybercrime? How has the digital age become a bonanza for organized crime? Which governments provide safe haven or even worse engage in state sponsored cybercrime? Joseph Menn, investigative journalist and author of *Fatal System Error,* will share his findings and answer your questions.

Speaker: Joseph Menn, Prize winning journalist for the *Financial Times* and the *Los Angeles Times*, author of *Fatal System Error*, *All the Rave: The Rise and Fall of Shawn Fanning's Napster*, and co-author of T*he People vs. Big Tobacco: How the States Took on the Cigarette Giants*. Joseph grew up in the Boston area and graduated with honors from Harvard College, where he was executive editor of *The Harvard Crimson*.

Afternoon Session I
1:30 p.m. – 2:45 p.m.

Krebs on Security: 60 Breaches and Counting.
For the past 16 months, Brian Krebs has been investigating a burgeoning form of organized cybercrime targeting small- to mid-sized businesses. To date, Krebs has broken more than 60 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, sophisticated malicious software, and a seemingly limitless supply of accomplices here in the United States and Europe.

Brian's talk will touch on all aspects of this crime – bringing you inside the operations of an organized cybercrime gang – and show you why victims' businesses are usually left holding the bag. The discussion also will shed light on the hundreds of "money mules" that are duped or lured each month into helping the criminals launder stolen money. Most importantly, Krebs will examine some of the ways that businesses and the financial industry can dramatically reduce the effectiveness of these criminals.

Speaker: Brian Krebs is editor of krebsonsecurity.com, a daily blog dedicated to in-depth cyber security news and investigation. Most recently, Krebs was a reporter for *The Washington Post*, where he covered Internet security, cybercrime and privacy issues for the newspaper and the website. In March, krebsonsecurity.com was named the best non-technical security blog at the RSA Security Conference, the world's largest annual computer security gathering.

Afternoon Session II
3:00 p.m. – 4:15 p.m.

Anatomy of an Attack: How Hackers Threaten Your Security
Gain insight into how attacks occur. This session is designed to show how chains of attacks link together both from the perspective of the hacker and the end user, showing in gory detail the true capabilities of modern malware. The highlight of the session will be a live malware attack in action (of course it will be self-contained so nothing to worry about there!).

Speaker: Dr. James Lyne, Chief Technology Officer, SOPHOS. With a strong background in mathematics and cryptography, and a detailed understanding of computer threats, James today studies key business and technology trends to map future security requirements at Sophos.

Afternoon Session III
4:30 p.m. – 5:30 p.m.

Respond and Defeat – Resources for Fighting Back
The criminals are well funded and determined; they are engaged in a low risk-high reward venture. It is time to fight back. This audience participation session will focus on what the ABA, Secret Service, FBI, and Department of Justice are doing to change the odds.

Speakers: Doug Johnson, ABA VP of Risk Management, Secret Service, FBI and Department of Justice crime fighters.

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

Dinner Keynote & Discussion
6:30 p.m. – 9:00 p.m.

Banking in Cyberspace: Managing the New Risks
Bankers have always been in the business of managing risks. James R. ("Jim") Woodhill, founder and chairman of Authentify, will give his perspective on the new risks that online banking has introduced. Fraud loss is an inevitable part of banking. In the world of online banking many institutions have chosen to do what Bruce Schneier has called "externalizing" the fraud costs–imposing it on the customers whose specific accounts were attacked. These decisions have reduced short-term financial risk, but have given rise to longer-term risks.

Customers are suing. Is there a risk that a court might soon rule and set a precedent that banks are indeed liable for all online fraud? But even if the courts rule for the banks, what of reputational risk? Might this reputational risk be "contagious" like the solvency risk that brought down not just Lehman Brothers, but the entire U.S. credit system with it two years ago? That is, might your bank suffer for what another bank "like" yours did and did not do? Come hear Jim Woodhill discuss the political risks the industry is taking and the options available to mitigate those risks.

Following Jim's presentation, the audience is invited to participate in a panel discussion on cyber-risk, political risk and regulatory reform. Moderated by Tom Field, Editorial Director of BankInfoSecurity, panelists include Jim Woodhill; Doug Johnson, VP Risk Management/ABA; former U.S. Representative James Longley, Jr.; and Dan Mitchell, Esq. Bernstein Shur.

NOVEMBER 5, 2010 • DAY TWO

Breakfast Keynote
8:00 a.m. – 9:30 a.m.

The Zeus Botnet: Stealing Everything from Millions of Americans
UAB Computer Forensics has worked closely with financial institutions, banking regulators, law enforcement, and the security research community to build an extensive profile of what Network World has called "The Most Wanted Botnet in the World." This presentation will document the structure, history, and strategies used to build a multi-million-node botnet for stealing not just banking credentials, but every item password and web form response on the infected computers. We'll discuss how this botnet is able to defeat even the most complex fraud detection and two-factor authentication techniques used today, and what that holds for the future of malware. This session was presented at the 2010 DOD CyberSecurity Conference.

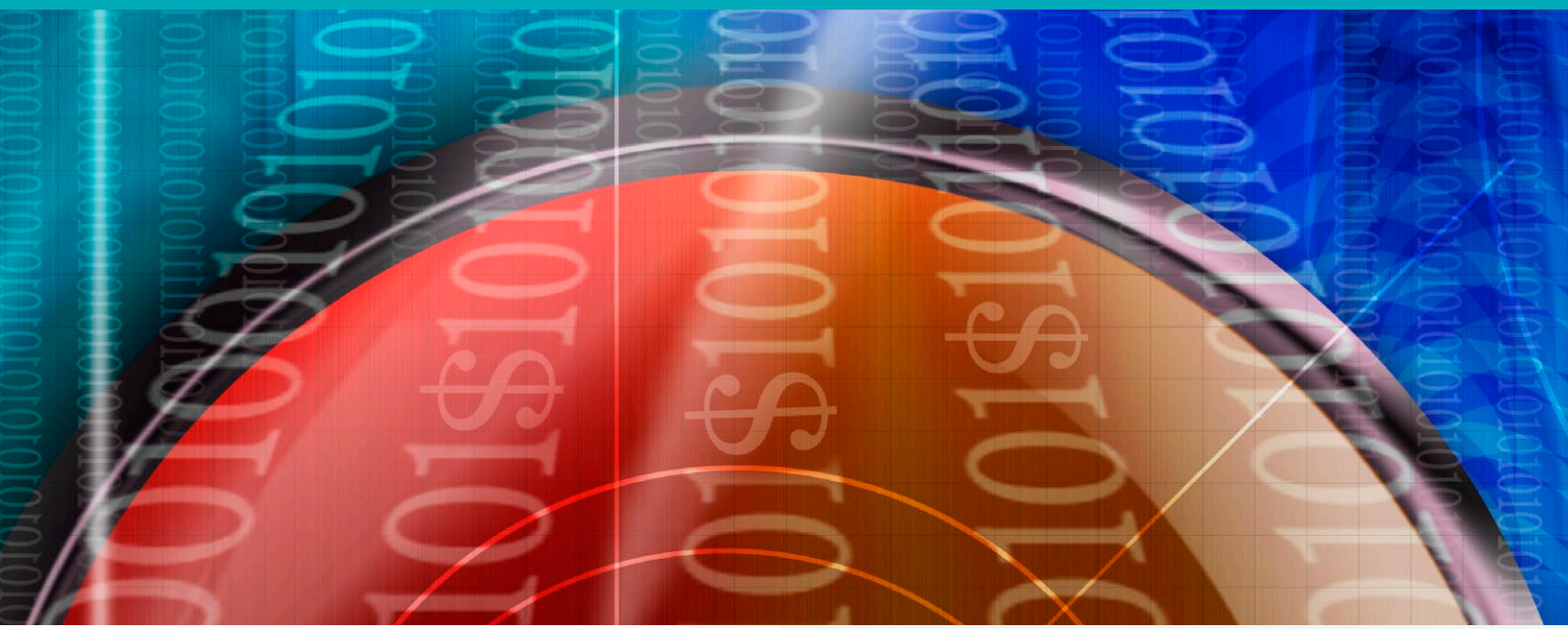
Speaker: Gary Warner, Director of Research in Computer Forensics, The University of the Alabama at Birmingham

Mock Cyber Security Incident Preparedness & Response Exercise
9:45 a.m. – 11:45 a.m.
Are you prepared to respond to a Corporate Account Hijacking? Is your customer? This audience participation simulation will walk you through a Corporate Account Hijacking event. Along the way, we will challenge ourselves and our institutional plans with the objective of ensuring that we are prepared to quickly react and respond in ways that minimize the financial, operational and reputation damage to both our institution and our customers.

Lunch and Closing Session
12:00 p.m. – 1:30 p.m.

Communicating with Customers
Successful cyber security requires layers of controls at the customer site, within Internet Banking and in the back office. This session will focus on how to communicate the inherent risk in online banking to customers without scaring or discouraging them, and educate them on their role and responsibilities. Sari has designed and presented this session to banking customers throughout New England. Joining Sari will be representatives of two New England Banks who tackled this challenge head on.

Speaker: Sari Greene, Sage Data Security
Panelists: Holly Young, Norway Savings Bank, and Arlene Stinson, Merrimack County Savings Bank



Responding to the Financial Cybercrime Epidemic

November 4–5, 2010

Sheraton Portsmouth Harborside Hotel | Portsmouth, NH

sage DATA SECURITY

About Sage Data Security

Founded in 2002, **Sage Data Security** is an information security firm located in South Portland, Maine. A strategic security partner for financial institutions, healthcare providers, government agencies and businesses nationwide, Sage is strongly committed to the principles of integrity, quality and commitment on both an organizational and personal level.

www.sagedatasecurity.com

noPhishing.org℠

About nophishing.org

nophishing.org is the action arm of the Maine Anti-Phishing Coalition (MEAPC), a group of 24 Maine banks created in 2006 with a mission of preventing information theft and fraud through public education and awareness. These member banks are committed to aggregating resources and sharing information.

www.nophishing.org

www.cybercrime2010.com