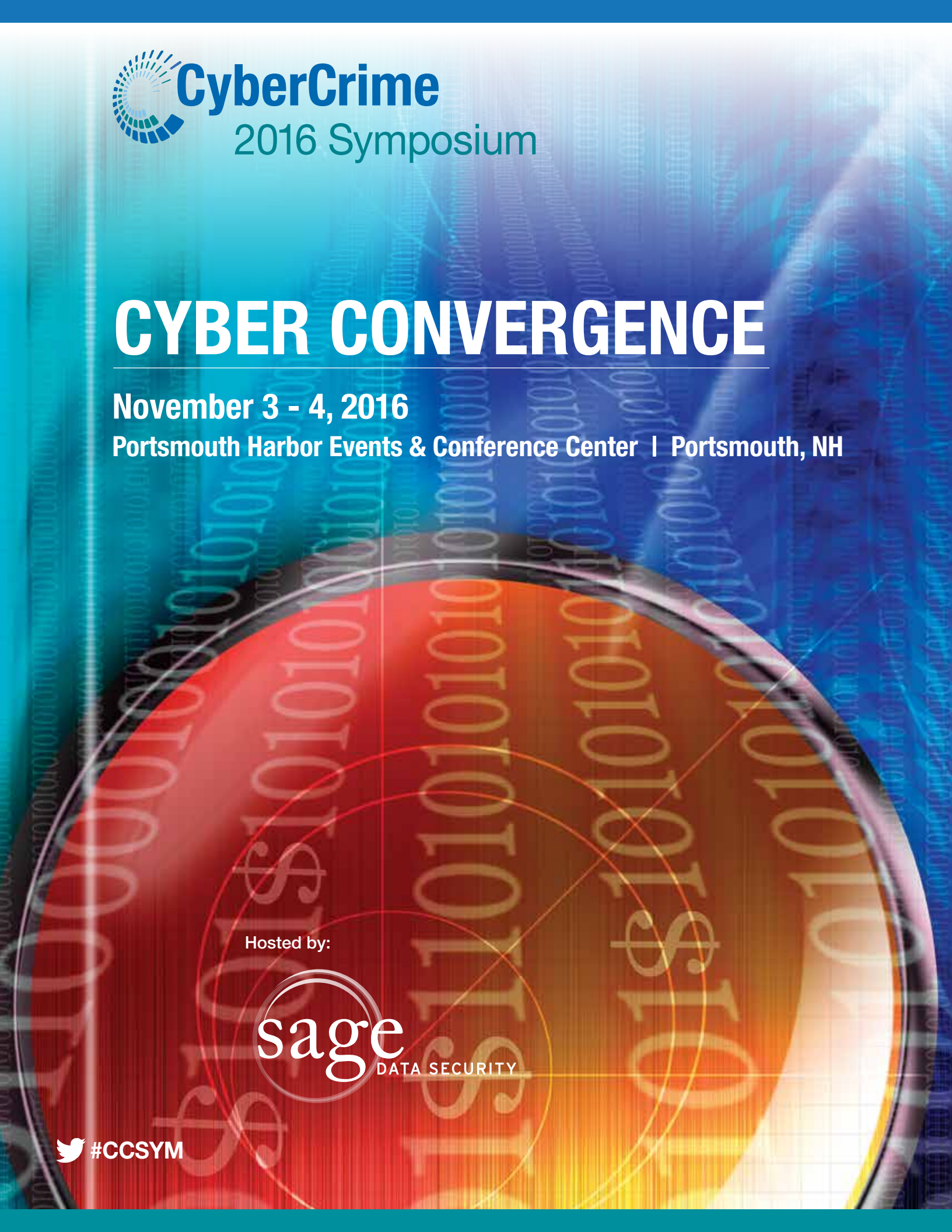
CyberCrime
2016 Symposium

CYBER CONVERGENCE

November 3 - 4, 2016

Portsmouth Harbor Events & Conference Center | Portsmouth, NH



Hosted by:

sage DATA SECURITY

#CCSYM

CyberCrime Symposium - 2016 Agenda

Program is subject to change.

DAY ONE: Thursday, November 3, 2016

Registration Opens: 11:30 a.m.

Box Lunch: 11:45 a.m. – 12:15 p.m.

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

Cyber Convergence

Sari Stern Greene, Sage Data Security Host Representative

Insider threats, cybercriminal attacks, and state sponsored hacks have become everyday occurrences. To protect our companies, communities, and countries, we must break down silos and take a integrative approach. The 2016 Symposium is about convergence and resiliency.

Sari Stern Greene, CRISC, CISM, CISSP-ISSMP is a cybersecurity practitioner, educator, and founder of Sage Data Security. She is the author of *Security Program and Policies: Principles and Practices*, as well as the best-selling CISSP Complete Video Course and the newly released CISSP Exam Prep Video Course. Sari serves on the Bangor Savings Bank Board of Directors, Mass Bankers Cybersecurity Task Force, and the ABA Cybersecurity Faculty. T: @sari_greene

Lunch Keynote: 12:15 p.m. – 1:15 p.m.

Cyber Breach: What if Your Defenses Fail? Design an Exercise to Map a Ready Strategy.

Regina Phelps, Emergency Management Expert, Educator, Author

Every month we read about the latest, the greatest, or "the most significant cyber breach ever." A cyber incident affects every aspect of the business, and has become one of the most pressing issues in crisis and business continuity management today. The goal of this session is to demonstrate the value of conducting cyber incident exercises. You will discover how a cyber incident exercise is different from other exercises and learn the eight critical elements of a successful cyber exercise. Most importantly, Regina will share with you how to design and implement an excise that will enhance your organizational resiliency.

Regina is an internationally recognized thought leader in the field of emergency management, pandemic, and contingency planning. Since 1982, she has provided consultation and speaking services to clients in four continents. She is the founder of Emergency Management & Safety Solutions (EMSS), a consulting and training firm that is 100% woman owned. A partial listing of clients include: Northern Trust, LexisNexis, Whole Foods Market, McAfee, Duke University, the World Bank, Microsoft, Stanford University, VISA, Principal Financial, Caltech Institute, Wells Fargo, Sentry Insurance, MasterCard, PG&E, International Paper and American Express. T: @reginaphelps

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

Demystifying a Malware Attack

Christopher Elisan, Principal Malware Scientist, RSA

The media reports different malware attacks, different lamentations from those affected, and different opinions of industry experts. What is lost in the conversation is the background: how are these attacks started, what are the different recipes of successful attacks, and who are behind them. Christopher will present an inside look at what goes on in an attack and the different technologies and people involved.

Christopher is a seasoned reverse engineer and malware researcher. His long history of digital threat and malware expertise, reversing, research, and product development started at Trend Micro as one of the pioneers of TrendLabs, where he honed his skills in malware reversing. He then built F-Secure's Asia R&D where he spearheaded projects in vulnerability discovery, web security, and mobile security. After F-Secure, he joined Damballa as their resident malware subject matter expert and reverse engineer. He speaks at conferences around the world and frequently provides expert opinion about malware, botnets, and advance persistent threats for leading industry and mainstream publications. T: @Tophs

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

Malware Activity in Mobile Networks: An Insider's View

Kevin McNamee, Director, Nokia Threat Intelligence Lab

Kevin's talk will explore the malware that is currently active on the mobile network and will leverage aggregated data from live network deployments of Nokia's NetGuard EndPoint Security system, a network based malware detection system deployed in mobile carriers covering more than 100 million mobile devices around the globe. He'll start with a review of real world malware statistics for mobile devices, and then provide an in-depth analysis of specific malware infections, including details on what the malware does, its command and control infrastructure, how it is monetized, and the impact on the network and user.

Kevin McNamee, the Director of Nokia's Threat Intelligence Lab, is a seasoned IT security professional with more than 30 years of experience. Previously at Alcatel-Lucent he designed their cloud-based malware detection system and was director of Security Research with Alcatel-Lucent's Bell Labs, specializing in the analysis of malware propagation and detection. Kevin has also managed product development of Milkyway's Blackhole Firewall and TimeStep's IPSEC VPN product, and he was Director of Research & Development for Alcatel's OmniAccess/ IPSEC products. He is the primary author of the Nokia Threat Intelligence Report and has had several recent speaking engagements at Black Hat, RSA, SECTOR and ISC^2.

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

Bitcoin's Not the Cause of Ransomware, but It's Raising the Stakes.

Peter Van Valkenburgh, Research Director, Coin Center

There are three things that make ransomware possible: breach, encryption, and payment networks like Bitcoin. Encryption and Bitcoin are the "sexy" parts of that trifecta, and accordingly they get most of the media attention. But the root problem is breach and the poor security practices that lead to breach. This talk will look specifically at the rising problem of ransomware, how Bitcoin plays a role in that rise, and — more broadly — how cryptocurrencies are raising the stakes in computer security and computer crime.

Peter is the Director of Research at Coin Center, the leading non-profit research and advocacy group focused on the policy issues facing cryptocurrencies like Bitcoin. He is a graduate of NYU Law, as well as a self-taught designer and coder. Peter drafts the Center's public regulatory comments and helps shape its research agenda. He has briefed policymakers and regulatory staff around the world on the subject

of Bitcoin regulation. Previously, he was a Google Policy Fellow and collaborated with various digital rights organizations on projects related to privacy, surveillance, and digital copyright law. T: @valkenburgh

Afternoon Session IV: 5:00 p.m. – 5:30 p.m.
New England Cybercrime Town Hall

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

The Secret Service is committed to safeguarding the nation's critical infrastructure and financial payment systems from cyber criminals. SSA Matt O'Neil will brief us on recent New England cases and investigations and invite questions and observations from attendees.

Matthew O'Neill won the Department of Homeland Security Silver Medal in 2014 and the USSS Special Agent of the 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. SSA 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. – 7:00 p.m.

Dinner Keynote: 7:00 p.m. – 8:00 p.m.
Getting and Staying CyberSmart: Resources and Breaking CyberBread

Christina Ayiotis, Esq., Cybersecurity Advocate and Cross-Pollinator

Understanding how to properly protect valuable information assets in today's data-driven, interconnected global economy often involves working with multiple parties. The Cybersecurity Canon, a listing of vetted books, offers resources for context in this ecosystem. Given the exponential speed of change in cybersecurity, continuous learning is the only viable strategy to stay CyberSmart. Such learning can come from written resources, but also must include active human collaboration. This session will enable you to strategize about how to create the network and knowledge to stay ahead of the threat.

Christina, an internationally-recognized leader in cyber, privacy, data protection, and electronic discovery, serves as Co-Chair of the Georgetown Cybersecurity Law Institute and is a Member of both AFCEA International's Cyber Committee and The Cybersecurity Canon Committee. She taught Information Policy at George Washington University and served as Deputy General Counsel — Information Governance, at CSC, a global technology services provider. She also led global programs at Booz Allen Hamilton, EYI, and Deloitte Touche Tohmatsu. She served on the Boards of ARCS MWC, Fairfax Law Foundation, ARMA NOVA, Hellenic American Women's Council, and Women's Bar Association of DC. T: @christinayiotis

Evening Entertainment: 8:30 p.m. – 10:00 p.m.

Socialize and unwind. Join us across the street at the Hampton Inn and Suites lobby and enjoy some local entertainment and cash bar.

Share your CyberCrime insights on twitter using #CCSYM

DAY TWO: Friday, November 4, 2016

Breakfast Buffet: 7:30 a.m. – 8:00 a.m.

Federal Reserve Special Session (optional): 7:30 a.m. – 8:00 a.m. in the Spinnaker Room

Join us for this special mini-session with Don Anderson, Jr., the SVP and CIO at the Federal Reserve Bank of Boston, who will discuss how the Fed is leveraging the cloud for information security.

Breakfast Keynote: 8:00 a.m. – 9:00 a.m.
The Internet of Threats: Billions of Ways the IoT Poses an InfoSec Challenge

Chris Poulin, Research Strategist, X-Force at IBM

Many IoT devices are hidden from view and pose a threat to your IT systems and even their physical safety — and that of the humans that tend to them. You may not own the HVAC system or the elevators in your building, but you're going to want to connect them to your Exchange server. And that new connected car in the parking lot that doesn't seem to be dangerous to your data could well be the newest means of exfiltrating data. In his session, Chris will present use cases that break down the barriers between IoT devices and IT assets — and explain why they're inevitable — and present strategies to prepare for the inevitable rise of SkyNet.

Chris is an engineer and entrepreneur, having built and run a nationally respected information security consulting firm that provided services to companies from Fortune 500 to small businesses. With 25 years in information technology and security, he's successfully managed hundreds of projects in practically all industries, bringing a balance of technical skills and management experience, as well as unique experience from his time in the Department of Defense intelligence community. Chris' current passion is the intersection of digital security and the physical world. Oh, and he picks locks in his spare time. T: @ChrisPoulin

Morning Session I: 9:15 a.m. – 10:00 a.m.
ICSA Labs: Defending Against Unknown Threats

Jack Walsh, New Initiatives and Mobility Programs Manager, ICSA Labs

Defending your network from breaches requires a defense-in-depth strategy. Even with all the traditional security defenses, breaches still occur due in part to the fact that there's been no real answer for new threats. Enter advanced threat defense (ATD) solutions. For 25 years ICSA Labs has performed computer and network security certification testing. Jack will explain how they are testing ATD solutions, the most recent findings, and how you can benefit from ICSA's ongoing testing and research.

Jack has been with ICSA Labs, an independent division of Verizon, for 18 years. and is currently driving development of programs that test the security of IoT devices, advanced threat defense solutions, and all things mobile. Jack's prior roles included network intrusion prevention systems program manager, anti-spam program manager, and firewall lab technical lead. Previously, Jack tested commercial products at the National Security Agency. While there he co-authored the first Firewall Protection Profile.

Morning Session II: 10:00 a.m. – 10:45 a.m.
The Trusted Insider

Don Ulsch, Sr. Managing Director Cybercrime & Breach Response, PwC

Statistically, regardless of the size of your company, an information breach will originate with a trusted insider. That trusted insider may be an employee,

a contractor, or even a third-party vendor. Because insiders are, in fact, "trusted," they pose a special threat. Using case histories, Don will discuss various companies that were breached by trusted insiders, and what you can do to mitigate the risk to your organization.

A specialist on cybercrime, Don rejoined PricewaterhouseCoopers LLP in 2014. Working with many well-known corporate brands, as well as law enforcement and the intelligence community, he has led many complex cyber breach investigations and advised executive management on breach management strategy and mitigation execution. Don is the Chair of the American Bar Association Criminal Justice Section Cyber Crime and Privacy Subcommittee. He has appeared on ABC News and Fox News as a cybercrime and breach analyst. He served as a national security advisor to *The DaVinci Code* author, Dan Brown.

Morning Session III: 11:00 a.m. – 12:00 p.m.
Cyber Who Done It?! Arrest History Attribution Analysis

Jake Kouns, CISO, Risk Based Security; CEO, Open Security Foundation

Arrest history and analysis of data breaches paint an interesting picture of the cybercrime landscape. Jake will present current research and his observations, including who is behind these data breaches and what the demographics are, how many work by themselves versus part of a group, which day of the week are you most likely to be arrested, and how many arrests lead to assisting authorities to arrest others.

Jake is the CISO for Risk Based Security and the CEO of the Open Security Foundation that oversees the operations of the Open Source Vulnerability Database (OSVDB.org) and DataLossDB.org. He has presented at many well-known security conferences including RSA, DEF CON, and IEEE GlobeCom. Jake holds a number of certifications including CISSP, CISM, CISA and CGEIT. He has also been interviewed as an expert in the security industry by several industry publications, including CNN, Information Week, and SC Magazine. T: @jkouns

Lunch Buffet: 12:00 p.m. – 12:30 p.m.

Lunch Keynote: 12:30 p.m. – 1:30 p.m.
Implementing Gamification and Other Creative Security Awareness Methods

Ira Winkler, CISSP, CyberExpert, Educator, Author

If we're going to take hacking seriously, what needs to happen is 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.

Ira is President of Secure Mentem, co-host of The Irari Report, and ComputerWorld columnist. He is considered one of the world's most influential security professionals, and has been named a "Modern Day James Bond" by the media. He did this by performing espionage simulations, where he physically and technically "broke into" some of the largest companies in the world and investigated crimes against them. Then told them how to cost effectively protect their info and computer infrastructure. He continues to perform these espionage simulations, and helps organizations develop cost-effective security programs. Ira has won several prestigious industry awards. Most recently CSO Magazine named him The Awareness Crusader, a CSO Compass Award. T: @irawinkler

Afternoon Session I: 1:45 p.m. – 2:30 p.m.
Compromising Merchants: A Live Hacking Demo

Gary Glover, Director of Security Assessment, SecurityMetrics

Merchant data is continually under attack. But how? What makes them vulnerable? The Live Hack Demo helps technical and non-technical audiences understand how easily unprotected credit card data can be stolen. This demonstration covers past compromises, hacking methodology, live hacking examples, and tips to implement the PCI Data Security Standard.

Gary Glover is the Director of Security Assessment at SecurityMetrics and holds QSA, PA-QSA, CISSP, and CISA security certifications. Gary has worked in the IT security industry as a QSA for over 10 years. Before that, Gary spent 10+ years as a software engineer at Novell, McDonnell Douglas, and other startups. Gary is the author of two US patents, and received a Masters of Science in Mechanical Engineering from Brigham Young. T: @G2glvr

Afternoon Session II: 2:30 p.m. – 3:15 p.m.
Got Coverage? Cyber-Insurance Realities Revealed

Peter Foster, Executive Vice President, FINEX Cyber/Tech E&O, Wilson Towers Watson

Cyber-insurance is an important component of a risk mitigation strategy. Jacob will guide us through the intricacies of cyber-insurance including typical coverage features, most common exposures, purchasing process, loss examples, and the claims handling process. This is must know information for every organization!

Peter has sixteen years of experience providing risk solutions and strategic advice to large, complex corporations and financial institutions on privacy, network security (cyber) and technology errors & omissions risks and exposures. In his role as one of the Willis Towers Watson Cyber leaders, he is focused on providing strategic advice and risk transfer services to FINEX's large financial services, healthcare, retail and defense contractor clients.

Closing Remarks: 3:15 p.m. – 3:30 p.m.

Rick Simonds, Chief Operating Officer, Sage Data Security