Cyber Defense and Disaster Recovery Conference 2011: Securing the Human Speakers and Topics

---

Howard Schmidt, CISSP, CSSLP
Special Assistant to the President and Cybersecurity Coordinator

Howard A. Schmidt has had a long distinguished career in defense, law enforcement, and corporate security spanning more than 40 years. He brings together talents in business, defense, intelligence, law enforcement, privacy, academia and international relations through his distinguished career. He currently is Special Assistant to the President and the Cybersecurity Coordinator for the federal government. In this role Mr. Schmidt is responsible for coordinating interagency cybersecurity policy development and implementation and for coordinating engagement with federal, state, local, international, and private sector cybersecurity partners.

Previously, Mr. Schmidt was the President and CEO of the Information Security Forum (ISF). Before ISF, he served as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay Inc. He also served as Chief Security Strategist for the US-CERT Partners Program for the Department of Homeland Security.

Before eBay, he served as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House. Prior to the White House, Howard was Chief Security Officer for Microsoft Corp., where his duties included Chief Information Security Officer, Chief Security Officer, and forming and directing the Trustworthy Computing Security Strategies Group.

Mr. Schmidt is recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Mr. Schmidt's government experience includes work with the Air Force Office of Special Investigations (AFOSI) Computer Forensics Lab and Computer Crime and Information Warfare Division, the FBI at the National Drug Intelligence Center, and the Chandler Police Department in Arizona.

Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard as computer communications specialist from 1989 until 1998, when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division. where he served until 2010 with the computer crime investigations unit at CID HQ.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the University of Phoenix. He also holds an Honorary Doctorate degree in Humane Letters. Howard was an Adjunct Professor at GA Tech, GTISC, Professor of Research at Idaho State University and Adjunct Distinguished Fellow with Carnegie Mellon's CyLab and a Distinguished Fellow of the Ponemon Privacy Institute.

Video Message: "Our Shared Cybersecurity Responsibility"

White House Cybersecurity Strategy

What We Must Do

Our Nation's cybersecurity strategy is twofold: (1) improve our resilience to cyber incidents and (2) reduce the cyber threat.

Improving our cyber resilience includes: hardening our digital infrastructure to be more resistant to penetration and disruption; improving our ability to defend against sophisticated and agile cyber threats; and recovering quickly from cyber incidents—whether caused by malicious activity, accident, or natural disaster.

Where possible, we must also reduce cyber threats. We seek to reduce threats by working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of our remaining vulnerabilities.

Underlying all of these efforts is the need to acquire the best possible information about the state of our networks and the capabilities and intentions of our cyber adversaries. We must also make critical cybersecurity information available to and usable by everyone who needs it, including network operators and defenders, law enforcement and intelligence agencies, and emergency management officials in the Federal, State, local, and tribal governments, private industry, and allied governments.

As we take all these actions to secure our networks, we will do so in a manner that preserves and enhances our personal privacy and enables the exercise of our civil liberties and fundamental freedoms. In the 21st Century, our digital networks are essential to our way of life around the world and are an engine for freedom. We will lead by example in order to demonstrate that increased security, enhanced user privacy and keeping the Internet open and innovative go hand-in-hand.

Near Term Actions

The President's Cyberspace Policy Review identifies 10 near term actions to support our cybersecurity strategy:

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure.
2. Designate cybersecurity as one of the President's key management priorities and establish performance metrics
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Conduct interagency-cleared legal analyses of priority cybersecurity-related issues.
6. Initiate a national awareness and education campaign to promote cybersecurity.
7. Develop an international cybersecurity policy framework and strengthen our international partnerships.
8. Prepare a cybersecurity incident response plan and initiate a dialog to enhance public-private partnerships.
9. Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.
9. Build a cybersecurity-based identity management vision and strategy, leveraging privacy-enhancing technologies for the Nation.

http://www.whitehouse.gov/administration/eop/nsc/cybersecurity

Alex Hutton
Principal for Research & Intelligence, Verizon Business RISK Team

Alex Hutton is a big fan of trying to understand security and risk through metrics and models. Currently, Alex is a principal for Research & Intelligence with the Verizon Business RISK Team. The Verizon RISK Team builds and hones the risk models for Cybertrust services, produces the Verizon Data Breach Investigation, the Verizon's PCI Compliance report, and is responsible for the VERIS data collection and analysis efforts. As a member of the RISK team, Alex also writes regularly for the Verizon Security Blog (http://securityblog.verizonbusiness.com).

Alex likes risk and security so much, he spends his spare time working on projects and writing about the subject. Some of that work includes contributions to the Cloud Security Alliance documents, the CIS metrics project, the ISM3 security management standard, and work with the Open Group Security Forum. Alex is a founding member of the Society of Information Risk Analysts (http://societyinforisk.org/), and blogs for their website and records a podcast for the membership. He also blogs at the New School of Information Security Blog (http://www.newschoolsecurity.com).

In the 15 years before joining Verizon, Mr. Hutton served as an information risk and security consultant, serving companies from the Fortune 10 to the SMB market. He has also served as Product Manager for security product vendors, and as an executive in two security start-up companies.

Keynote: "Changing The Way We Do Risk Management: An Evidence-Based Approach"

Is there a disconnect between governance, risk management, and compliance (GRC) and operational security? Can compliance mandates impact "real" security? What are the enterprise implications of cybercrime statistics? As both an author of the Verizon Data Breach Investigations Report and a founder of the Society of Information Risk Analysts, Alex Hutton's unique perspective explains why risk management is inescapable, what's wrong with the way we currently view information risk management and security, and what our industry can do to create a more effective, evidenced-based approach.

Lance Spitzner
Technical Director, SANS Securing The Human Program

Mr. Lance Spitzner is an internationally recognized leader in the field of cyber threat research, security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world, for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project; an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

Mr. Spitzner has spoken to and worked with numerous organizations, including the NSA, FIRST, the Pentagon, the FBI Academy, the President's Telecommunications Advisory Committee, MS-ISAC, the Navy War College, the British CESG, the Department of Justice, and Monetary Authority of Singapore. He has consulted around the world, working and presenting in over 20 countries on 6 different continents. His work has been documented in the media such as CNN, BBC, NPR, and Wall Street Journal. He serves on the Distinguished Review Board for the Air Force Institute of Technology, Technical Review Board for CCIED, and the Information Assurance Curriculum Advisory Board at DePaul University. Before information security, Mr. Spitzner served as an Armor officer in the Army's Rapid Deployment Force and earned his M.B.A. from the University of Illinois-Chicago.

"SANS Security 464: Hacker Detection for SysAdmins Continuous Education Program"
For more information: http://bit.ly/SANS464program

Opening Session: Securing The Human

Organizations have traditionally invested most of their security in technology, with little effort in protecting their employees. As a result, many attackers today target the weakest link, the human. Awareness, not just technology, has become key to reducing risk and remaining compliant. This high-level talk designed for management explains why humans are so vulnerable, how they are being actively exploited and what organizations can do about it. Key points include:

- How humans are nothing more then another type of operating system, albeit a highly vulnerable one.
- Why humans are so bad at judging risk and how attackers exploit these vulnerabilities.
- How an effective awareness program patches these vulnerabilities and reduces risk.
- How to develop a modular and flexible program that reach multi-cultures.
- How to create and effectively use metrics.

Workshop Session 1 - Security Awareness Strategic Planning

Before you start a security awareness program, there are several key strategic issues you have to identify. We will cover the most important strategic issues, including:

- Defining the goals of your program
- Key players in a successful awareness team
- Building a business case and getting funding
- Developing materials in house or outsourcing
- Distributed model
- Resources for learning more

Workshop Session 2 - Security Awareness Communication

The key to any successful security awareness program is communication. How you communicate your program will have a tremendous impact on how effectively you change behaviors. In this one hour presentation we will focus on how to ensure your communication is a success, including:

- Top ten steps to a successful presentation and top five most common mistakes to avoid.
- Advantages of on-site versus online training.
- What an LMS is and how it works
- Resources for learning more

Mike Bazzell
Detective, Alton Police Department, FBI Metro East Cyber Crimes Task Force

Mike Bazzell is the Computer Crime Detective for the Alton Police Department, and currently handles all cases involving any type of Computer Crime and Computer Forensic Analysis, including several State and Federal cases throughout the Metro-East St. Louis area.

Upon completion of his degree in criminal justice, he was selected as the Director of the Metro-East Regional Computer Crime Enforcement Group under the authority of the Illinois Attorney General. He currently instructs Computer Forensics and Ethical Hacking for Lewis & Clark College. He is also an active member of the elite Technical Operations Group of the Major Case Squad of Greater St. Louis. In 2005, Mike was assigned full time to the FBI's Cyber Crime Task Force, where he continues to assist with Federal cases being prosecuted by the United State's Attorney's Office. As an active member of these organizations, he has been involved in numerous high-tech crime investigations including online child solicitation, manufacture of child pornography, child abduction, kidnapping, cold-case homicide, and internet bank intrusions. In his free time, he is a published photographer, author, and studio musician.

"The End of Privacy - Personal Information on the Internet"

This presentation identifies many unknown repositories of personal information available to anyone on the Internet. Through data mining companies and those that post personal information about others, data once considered private is now public. This look at our new lack of privacy will surprise even those that think they are not vulnerable. Over 120 sources of online information will be discussed. Aside from web sites, other technology such as digital camera data, document meta data, and files being unknowingly copied to your computer will be explained.

Dr. Faith M. Heikkila, PhD, CISM, CIPP
Chief Information Security Officer, Greenleaf Companies

Dr. Faith Heikkila is Chief Information Security Officer for Greenleaf Companies. She is responsible for overall information security governance and compliance, and oversees the protection of personal and financial information for clients of the Greenleaf Companies, which include Greenleaf Trust, Greenleaf Hospitality Group and Catalyst Development Company. Dr. Heikkila is also the Michigan InfraGard Member Alliance President. Previously, Dr. Heikkila gained over 18 years of paralegal and IT project management experience at two large law firms in Michigan.

Dr. Heikkila earned her Ph.D. in Information Systems from Nova Southeastern University specializing in Information Assurance. Dr. Heikkila is a Certified Information Privacy Professional (CIPP) and a CISM (Certified Information Security Manager). She also holds a Graduate Certificate in Information Assurance: System Administration in Information Security and a FEMA IS-00860 Introduction to the NIPP Certificate.

Dr. Heikkila is the author of the e-discovery published works: "e-Discovery: Identifying and Mitigating Security Risks in Litigation" published in the IEEE IT Professional and the "Laws and Regulations: e-

Discovery" chapter in the Encyclopedia of Information Assurance.

Dr. Heikkila is widely recognized as a subject matter expert in e-discovery, data privacy, information security, information security policies and procedures, computer security breaches, HIPAA, HITECH Act regulatory compliance, financial regulatory compliance laws, and state data breach notification laws. In recognition of her authority in this burgeoning field, Dr. Heikkila's expertise is globally sought through publications, invited lectures and presentations, and in organizing regional conferences.

"e-Discovery and the Human Element"

This presentation will shed light on individuals' prolific use of electronically stored information (ESI) on a daily basis and its affect on e-discovery preparedness best practices. ESI must be produced in response to a lawsuit e-discovery document request, which potentially impacts the security of company data. An e-discovery policy can be customized to meet the business requirements of the company and outline ways to deal with the human aspect of e-discovery while preserving responsive ESI. This session will discuss legal holds, the impact of e-discovery on IT, how to develop a proactive approach to e-discovery, including the steps every organization must take regarding mitigating the human element through security awareness and policy compliance training.

David Johnson
Executive Director, Center for Advanced Defense Studies

Lt. Col. Dave Johnson (U.S. Army Retired) is a 1984 graduate of the United States Military Academy at West Point, a graduate of the Command and General Staff Course, the Joint Defense College (France), holds a Master's degree in the History of Strategy from La Sorbonne (Paris), and is a PhD Candidate (ABD) with the Centre de Recherche en Informatique at the University of Paris in Cognitive Informatics.

A distinguished Special Forces combat veteran, Dave's 22 year career is documented in the Congressional Record (E1384, 12 JUL 06). He served most recently coordinating Army logistics for Special Operations Forces as Chief of the Special Operations Theater Support Element- Central Command. An Army Strategist, his works have been published in professional military journals and are being used in instruction at the U.S. Air Force Staff College, Maxwell AFB, Alabama and The U.S. Army Command and General Staff College, Fort Leavenworth, KS.

After retiring in September 2006, Lt. Col Johnson joined the Intel Corporation as Director, Digital Security Products in the Middleware Division. He received a Division Recognition Award for his part in the development of the first Intel® VPro desktop platform. Coordinating the work of engineering teams in Argentina and China, he directed security input to development and marketing of the Intel® SOA Security Toolkit and the Intel® XML Software Suites. Dave was a founding member of the Intel Security Architects Forum, Security Planning Forum, and Security Marketing Forum. He was also corporate lead for the cross-business unit participation in the 2008 RSA Conference.

Leaving Intel in 2009, Lt. Col. Johnson became the third Executive Director of the Center for Advanced Defense Studies in a ceremony at Grand Central Station, NYC. There, he continues to lead Cyber Security research and push policy issues.

“Segmenting Threat: Intent-Centric Security”

Securing the human is unattainable with even the best education programs, psychological profiles and tools. An old military axiom is that he who defends everything, defends nothing. While cyberspace provides unique opportunities and threats, humans act based upon their intent. These intentions can be segmented to identify effect and probability. The nature of the threat then drives the security effort. Examples discussed will include spear-fishing attacks, SQL injections, DoS attacks, and bot nets. Finally, to better identify the types of threats and probability for consumers I would make some high level policy recommendations.

Steffan Nass
Weapons of Mass Destruction Coordinator, Federal Bureau of Investigation

Special Agent Steffan Nass entered on duty with the FBI in 1996 and was assigned to the Miami Division, where he investigated general criminal matters and public corruption. In 1999 he joined the Miami Division HazMat Team and later participated in the 2001 anthrax evidence collection and investigative efforts. SA Nass was transferred to the Springfield Division in 2005 where he currently serves as the division’s Weapons of Mass Destruction Coordinator.

SA Nass speaks regularly throughout the area regarding WMD matters, serves as an presenter at the FBI Academy New Agent’s Training Program and as a presenter with the FBI’s International Counterproliferation Program.

SA Nass is a 1986 graduate of Iowa State University (B.S. Mathematics), is married and has three children.

“WMD Primer for Private Industry”

An historical overview of WMD terrorism, current WMD threats and vulnerabilities, and a brief case study outlining the impact such an event can have on private industry.

Ken Pappas
CEO, True North Security Inc.

Ken Pappas is a recognized expert on network and data security for personal and business threat protection. As a sought-after Security Evangelist and public speaker, Ken has appeared on NBC TV and Radio stations speaking on Cyber terrorism and has been featured in Fortune, the Wall Street Journal, Tech News World, S.C. Magazine, and many others around the world.

“Knowing More About Threats, Risks and Compliance”

How valuable would it be if you had more of an understanding of the cyber threats, risks and security regulations? Learn how hackers are gaining entry into your networks and personal data and what countermeasures you can take today to prevent it. I will provide an update on the threat landscape and commentary on what is causing the rise in cyber crimes, highlighting examples of clever ploys using social media sites as a means to lure you into “accepting” malware, spyware and viruses. What you will

find most interesting is my predictions on tomorrow's threats and what actions you can take today to possibly protect your network and data from a breach.

Key takeaways include:
- Where Cyber Crime is growing
- What's driving the rise in cyber crime
- Why yesterday's technology failing
- The top security change drivers of 2011 and what actions to take now to stay ahead of the curve
- How to create an effective defense-in-depth strategy
- How to understand the latest threats and their implications
- Newer Web 2.0 threats and so much more

Suzanne Phegley
ATM/Fraud Investigator, FCB Banks

Suzanne Phegley is a fraud investigator for FCB Banks in southern Illinois. She has 16 years of experience in the financial industry with the last 10 years focused on ATM/Debit card fraud. She has worked with several law enforcement agencies on debit card cases. She is a founding member of the Tri County Financial Fraud Coalition (TCFFC) and belongs to several other local and nationwide organizations that help identify and mitigate fraud. She promotes Identity Theft by educating the general public with informative presentations.

Jim Pettitt
Director, ATM Security Strategy & Planning, Diebold Incorporated

Jim Pettitt joined the Diebold Security Group in 1976. Throughout his career Jim has held several positions in the areas of security and self-service including product and services development and global marketing. In his current position, Jim is responsible for the strategy and planning for ATM security and fraud portfolio of solutions. Jim holds a bachelors degree from the University of Akron.

"My card was used WHERE?"

A brief overview of a credit/debit card transaction and how it can be compromised. We will explore some current fraud trends that are happening. The presentation will give some examples of skimming devices on ATMs and steps that you can take to reduce your exposure.

Brad Ware
Community Outreach Specialist, Federal Bureau of Investigation

Brad Ware is the Community Outreach Specialist for the FBI Springfield Division. The Community Outreach Program is designed to enhance the public's trust and confidence in the FBI in order to enlist the cooperation and support of the community in our common interest to fight criminal activity, including the topics, cyber crime and preventing crimes against children. In this format we can open a new line of communication to help make the FBI more responsive to the community's concerns.

“FBI-SOS (Safe Online Surfing) Internet Challenge”

This is a FREE, online, educational program that promotes cyber citizenship among students by engaging them in a fun age-appropriate, competitive online program where they learn how to safely and responsibly use the Internet. The program is designed for students in grades 3 through 8.

Chris King
Director of Product Marketing, Palo Alto Networks

Chris previously held strategic and product marketing roles at Blue Coat Systems, including responsibility for marketing and strategy for MACH5, Blue Coat's application acceleration solution, which he launched and helped grow to a $160 million/year business. Prior to joining Blue Coat, Mr. King spent more than eight years as an information technology analyst for META Group. An internationally recognized expert on information security, Mr. King has consulted with hundreds of large IT organizations, spoken before a variety of audiences, and is often quoted in trade and business press.

“Securing Access to Applications and Social Media”

Traditional firewalls sit at the perimeter and do little more than filter incoming packets, with simplistic rules. They are cumbersome and do a poor job of protecting web applications and social media websites. Employees and business partners need flexibility in accessing what they need, when they need it, and they need to know their data is well-secured against attacks. A new generation of firewall technology is more extensible and makes "intelligent" choices, so the right people have the access they need, from anywhere, at anytime. Policy-based decision-making at the firewall is now possible, because of faster hardware that allows the high-thoroughput and low latency that business users demand. This new generation of firewall technology is needed, as the corporate perimeter erodes and the distinction between what is internal and external becomes blurred.
