Cyber Defense and Disaster Recovery Conference 2012: IT Evolution's Societal Impact

Presentations & Speakers

Opening Remarks

Dr. Susan Koch, Chancellor, University of Illinois at Springfield
David A. Ford, Special Agent in Charge, FBI Springfield Division

Keynote Presentation - "Accepting and Building a 'Bend But Don't Break' Defense"

One philosophy in designing a defense in football is to focus significantly on not allowing the offense to gain yards. You play aggressive at the point of attack, focus on the battle in the trenches, and frequently try to out maneuver the opponent. The results can be stellar when your team is more athletic than the opponent; however, that same approach can be disastrous when you play a team with talented players who can scramble from the pass rush, run through tackles, and win the battle for jump ball passes down the field. That is why defensive coordinators at most every level have come to accept the fact that some offensive teams are going to make good plays and are going to gain yards. These coordinators live with a "bend but don't break" mindset where they protect what they value most (their end zone), and they try to win the most crucial battles at the most critical times.

This talk will draw comparisons between the security posture of an organization and the defensive game plan of a modern football team. Being completely successful at keeping adversaries out of your network is similar to trying to hold the best NFL quarterbacks to less than 250 yards throwing in a game. Quite simply, you just cannot do it 100% of the time.

In this talk we will size up the most talented adversaries, and we will discuss why older defensive approaches do not protect you from these sophisticated attackers. We will also discuss what a "bend but don't break" defense looks like in the world of information security. It starts with an acceptance that at times you will get compromised and that you need to have to a plan to deal with that fact. Three main elements to a successful defensive game plan will be described: visibility, intelligence, and an ability to respond.

Dan McWhorter, Director of Professional Education, Mandiant

Keynote Presentation - "Your Automobile, the Rolling Computer: Risks and Rewards"

Will provide information intended to stimulate thoughts about how the evolution of the computer and automobile have intersected to enhance the life style for today's consumer. The discussion will evoke thoughts by each professional on their opportunity to further this evolution through their own participation in developing solutions to technical challenges.

Rod Kinghorn, General Director of Global Security, GM Global Security Operations

SANS Track

For the third consecutive year, we are fortunate to be able to offer a SANS track with the generosity of SANS. This track has three parts, an opening session and two lab sessions. You are required to attend the opening session, which begins earlier than the normal conference starting time, to be able to attend the lab sessions. You may attend each of the lab sessions in either order, according to your preference and other conference presentation selections.

SANS Opening Session - "If I Were Evil: Why every organization's network has been breached"

SANS Lab Session 1 (Hands-on workshop) - "Malware: How Anyone Can Create a Zero Day Exploit in Less than 15 Minutes"

SANS Lab Session 2 (Hands-on workshop) - "Easily Detecting Malware and Persistent Intrusions with Script Creation for Baseline Monitoring"

Mick Douglas, Vice President, Systems & Data Security at Bank of America, Columbus, OH

Presentations & Speakers — Presentation Sessions

"Business Continuity / Disaster Recovery Best Practices and Lessons Learned"

Business Continuity and Disaster Recovery practices require a holistic approach to Technology Risk Management. This session will build a case supporting the criticality of using effective technology recovery practices when planning for Business Continuity and Disaster Recovery requirements. Discussions of best practices and lessons learned will be emphasized throughout the presentation. Disasters take many forms and the best protection is knowing how to respond and being prepared.

Erich Spengler, Executive Director, Center for System Security and Information Assurance (CSSIA)

Robert West Thomas Jr., Chief of Information Technology for the Midwest Region and the Regional Security Manager, DHS Federal Emergency Management Agency

"Pacman"

Discussion and Q&A with a Pacman engineer about how Pacman almost never made it to market! What would the 80's have been like without Pacman?

"Virtualization — the Kane County Experience"

A presentation and discussion about the planning, implementation, testing and overall experience of virtualizing the IT infrastructure of a county as large as Kane County.

Anthony Franklin, Public Safety Systems Manager, Kane County Information Technologies Department

"FBI Cyber Jobs" (Note: 30 minute mini session, paired with Pacman)

Ever thought about joining the FBI? Want to know what it takes and how to get started? Come ask the FBI Springfield Applicant Coordinator, Special Agent Terry Moody and FBI Cybercrime Investigator, Special Agent Chris Trifiletti.

Special Agent Terry Moody , FBI Springfield Applicant Coordinator, Federal Bureau of Investigation

"You Don't Need Cyber to Defeat Cyber"

Computers and microprocessors are showing up in all kinds of devices. Bad guys aren't, however, required to attack cyber-based systems with cyber methods. Often physical or electronic attacks are quicker, cheaper, harder to detect, and require less technical sophistication on the part of the adversary. This talk will give examples of this idea from the work of the Vulnerability Assessment Team at Argonne National Laboratory. Devices and technologies to be covered include electronic voting machines, biometrics and other access control devices, locks, tags, seals, GPS, RFIDs, and microprocessor-based systems. Suggestions for better physical security for IT will be offered.

Roger G. Johnston, Ph.C., CPP, Vulnerability Assessment Team, Argonne National Laboratory

"Social networking: A Great Place to be Found by More than Just Your Friends"

The ubiquity of computing power, including mobile devices, has fostered the rapid pace of growth and usage of social networking sites and applications. This presentation will reveal some of the unintended ways your information may be used by others.

Jeff Thompson, Certified Expert Penetration Tester, Central Management Services, State of Illinois

Presentations & Speakers — Presentation Sessions

"The Direct and Indirect Impact of Hacktivists"

In September 2011, the Department of Homeland Security warned the members of a certain hacking collective are increasingly interested in attacking industrial control systems used to automate machinery used by factories, power stations, water treatment plants, and other facilities critical to national security. "Hacktivists" such as these have also demonstrated the ability to cause nuisance and actual physical and financial damage to many high-profile targets including government agencies, financial services sector companies, and energy entities.

While these far reaching exploits certainly affect us all in that they affect key aspects of our infrastructure and society, have you considered the effect of a similar attack, even if much smaller in size, against your business or personal interests? The hacktivists are using the power of the Internet to cross-train each other and encourage new members of their collective and in doing so have likely shortened the time needed to develop sufficient tactics, techniques, and procedures to disrupt any new interest they may have. Take the time now to consider your risk and shore up your defenses.

Jeffrey Pricher, Director of Information Security Engineering, Savvis

"Cyber Terrorism in Illinois – The Cyber Hack that Wasn't and What You Should Still Do About IT"

The chaos of cyber incident response is at best, difficult, and at worst debilitating to a business or individual. Last fall, an apparent cyber terrorism attack at a Springfield area water utility garnered international news headlines but the premise upon which the news reporting was based was not true. Learn how the utility worked together with law enforcement to weather the media storm, vet their cyber systems, and keep the water flowing. Key takeaways will allow you and your business to plan for an information technology attack, real or imagined.

Chris Trifiletti, Special Agent, Federal Bureau of Investigation

"So, You Think You Can Log?"

Logging is more than just pulling a bunch of logs together. Find out what is required to not only get the log data that provides useful information, but also a monitoring and management program to correlate and act on the information produced from your security devices and applications.

Joe Zacharias, IT Security Specialist, Information Security Professional

Ben Blome, IT Security Specialist, Information Security Professional

Ben Blome, IT Security Specialist, Information Security Professional

A graduate of Eureka College, Ben has spent the last twelve years in IT at a Fortune 600 company. His varied IT background includes programming, system administration and network security. He currently serves as team lead of the Security Operations Center where he deals with enterprise logging, data loss prevention, digital forensics and pen testing. Ben is an ArcSight Certified Security Analyst (ACSA) and Tufin Certified Security Expert (TCSE).

Ben became a member of Infragard in September 2010. In 2011 he was a keynote speaker at the Digital Forensics Exercise where he presented on the use of EnCase in forensic cases. He is also a 2011 graduate of the FBI Citizens' Academy.

Mick Douglas, Vice President, Systems & Data Security at Bank of America, Columbus, OH

Mick is an Information Security professional with a strong technical background and the ability to craft and enforce policy.

He is particularly focused on large enterprise level systems and networks where high availability and strong enterprise wide security are both top requirement.

A graduate of The Ohio State University, Mick has been an IT professional since 1997.

Mick has been teaching SANS Security courses since 2008. He has taught classes on Hacker Techniques and Incident Handling as well as the SANS course on Auditing Systems and Networks.

Anthony Franklin, Public Safety Systems Manager, Kane County Information Technologies Department

Anthony manages the Public Safety Systems Support Group of the Information Technologies Department of Kane County, Illinois, which is a civilian position directly responsible for overseeing all electronic information systems operated by the Sheriff's Office, 911 Center and all Public Safety Agencies in the County of Kane. Anthony administers and maintains full access in the Law Enforcement Agency Data System (L.E.A.D.S.) and represents the Sheriff's Office regarding the needs and operations of electronic information networks and acts as liaison with other governmental entities, such as the ETSB and Information Systems Steering Committee. Kane County implemented New World Systems Public Safety software solution (Aegis – Corrections, CAD, Records, Civil and Patrol). Anthony manages all elements of the system. The Aegis public safety software solution integrates solutions for dispatch, mobile computing, field reporting, records management and corrections.

Roger G. Johnston, Ph.C., CPP, Vulnerability Assessment Team, Argonne National Laboratory

Dr. Johnston was founder and head of the VAT at Los Alamos National Laboratory (LANL) from 1992 to 2007 and moved the team to Argonne in October 2007. Roger has provided consulting, R&D, vulnerability assessments and security solutions for over 40 government agencies and private companies, including DoD, DOE/NNSA, the Department of State, the intelligence community, the International Atomic Energy Agency (IAEA) and Euratom.

Roger has authored over 115 technical papers and 60 invited talks (including keynote addresses) and holds 10 U.S. patents. Roger has won numerous awards and is often interviewed by the national and international news media for his views on security. Roger's R&D has received extensive national and international media attention including the Wall Street Journal (three times), R&D Magazine (four times), national wire services, Newsweek, various U.S. and international newspapers, radio/television stations and networks (BBC, CBC, VOA, NPR), and over 80 trade journals.

Rod Kinghorn, General Director of Global Security, GM Global Security Operations

Rod graduated from Michigan State University School of Criminal Justice in 1974 with a Bachelor of Science degree. Upon graduation, Rod worked with General Motors Security from 1974 until the present in a variety of positions. In addition to security-related functions, he also held positions where he was responsible for fire protection and prevention, plant safety and worker's compensation. A majority of his assignments since 1984 for GM have been in the field of investigations where he used an integrated business process to direct investigations that included; internal and external frauds, thefts, major policy violations, allegations of criminal activity, loss of proprietary information, forensic analysis of information systems, counterfeit automotive parts, health care fraud, workplace violence threats, and undercover drug operations in support of GM's Global Operations.

During his career Rod's participation in related professional organizations has included serving 10 years on the Nevada Safety Council Board of Directors, including seven years as the Vice President of Administration, Chairman of the Sierra Nevada Chapter of the American Society for Industrial Security (ASIS), advisor, Secretary, President and Chairman for the Michigan Chapter of Infragard, and Chairman for the Michigan State University Identity Theft business partnership. In 2004, Rod was honored as a recipient of one of the first Alumni service awards presented by the MSU School of Criminal Justice during a ceremony held in East Lansing, Michigan. He currently sits on the MSU Anti-Counterfeiting and Product Protection Program, (A-CAPPP), advisory board.

Born in Scottsbluff, Nebraska and raised on a farm near Morrill, Nebraska, Rod is married and has two married daughters that live with their husbands in Alexandria, VA and Orlando, FL.

Dan McWhorter, Director of Professional Education, Mandiant

Dan is responsible for Mandiant's Professional Education service line. In this role Dan focuses on curriculum development, course delivery, personnel management, and business development. As a Mandiant consultant, Dan provides analysis for both incident response engagements and proactive assessments.

Prior to joining Mandiant, Dan was an Assistant Executive Director with ManTech International. During his time there, Dan built a MD-focused ManTech International computer forensics and intrusion operations capability from the ground up that resulted in a fully accredited 10,000 square foot facility and a multi-million dollar contract base. Dan has experience supporting , supervising, and leading an elite team of forensic and intrusion engineers, as well as technical managers and administrative personnel.

Dan is a graduate of the National Security Agency's (NSA) three-year Cryptologic Mathematics Program. In addition to completing several mathematics courses during this program, Dan contributed technically to multiple NSA offices. He created exploits from public computer/network vulnerabilities, developed computer network operations tools, explored forensic attributes of computer operating systems and applications, coded algorithms to identify and extract nuggets of intelligence from massive data sets, evaluated commercially available executables and assisted in the determination of their security, and researched error correction and its use in specific hardware devices.

Dan has worked toward his doctorate in mathematics at the University of North Carolina. He has a Master's of Science in mathematics from the University of Cincinnati, and a Bachelors of Science in mathematics from Mount Union College (with minors in Physics, Astronomy, and Secondary Education). Dan has thousands of hours of classroom experience, he has published and presented on numerous technical topics internal to the National Security Agency (NSA), and he has presented at several technical conferences. Dan currently holds an active Top Secret government security clearance.

Jeffrey Pricher, Director of Information Security Engineering, Savvis

Jeff is a CISSP with nineteen years' experience in IT with over 10 years focused on information security. He possesses a detailed understanding of operating systems, network ports and protocols, TCP/IP, intrusion detection/prevention and the OSI model. Knowledge of netwok exploits, security best practices, defense in depth measures and incident reporting and handling procedures. Jeff has a BS in Management/Computer Information Systems, a MA in Computer Resources and Information Management and an MS in Network Security. Some of his previous jobs include an Intrusion Detection Technician for the Air Force Air Mobility Command, a Security Engineer for the Air Force Communications Agency an Information Systems Security Officer for Boeing and an Information Security Manager at KV Pharmaceutical. Jeff also serves part-time with the Missouri Air National Guard as a Cyber Operations officer in an Air Operations Center.

Cyber Defense and Disaster Recovery Conference 2012: IT Evolution's Societal Impact

Presentations & Speakers — Speakers

Erich Spengler, Executive Director, Center for System Security and Information Assurance (CSSIA)

Erich has more than 20 years experience in information systems and security. He holds an MBA from Loyola University and an MS in computer science from the University of Illinois. In addition, Erich has served as a senior lecturer and adjunct instructor at Northwestern University since 2007. He has served as the executive director and principal investigator for the Center for Systems Security and Information Assurance since 2003. Erich holds several industry and professional certifications, including the Certified Information Systems Security Professional (CISSP) certificate.

Jeff Thompson, Certified Expert Penetration Tester, Central Management Services, State of Illinois

Jeff has years of experience in performing vulnerability assessments, incident response and computer forensics. He is on the Information Security Team, responsible for assessing the cyber security of more than 12 Illinois state agencies. He has worn many hats including server admin, white hat, security awareness speaker and even a jester hat.

Chris Trifiletti, Special Agent, Federal Bureau of Investigation

Chris serves as the InfraGard Coordinator and Counterintelligence Strategic Partnerships Coordinator for the Springfield Division of the FBI. He has worked a variety of cyber and violent crimes cases across the U.S. and around the world. Chris has provided training and case assistance in over twenty-eight states and thirteen countries and has served on Interpol and G8 committees on Internet child exploitation and victim identification.

Robert West Thomas Jr., Chief of Information Technology for the Midwest Region and the Regional Security Manager, DHS Federal Emergency Management Agency

Robert supports FEMA's activities in a 6 state region. These responsibilities include managing the support of information technology; desktops, laptops, and servers, voice telephony; analog, digital, and VOIP, Local Area Networks and Wide Area Networks, wireless systems; cellular, HF, VHF, UHF, SHF, and satellite communications, information security, information assurance, COMSEC activities, personnel security, and physical security of FEMA facilities in the region. He is also responsible for coordinating interoperable disaster emergency communications between federal agencies, states, local and tribal entities.

Robert is also currently a member of the U. S. Army Reserve serving as the Senior Instructor/Writer for the 3/100th Signal Battalion, 3rd Brigade, 100th Division. He is responsible for developing courseware and instruction of entry level students and Senior Non Commissioned Officers. He teaches Information Assurance, networking, computer maintenance and support, server maintenance and support, and various radio and satellite systems.

Robert has also been serving on the National Visiting Committee for the National Science Foundation's Center for Systems Security and Information Assurance and has been a part of the Collegiate Cyber Defense Competition and on the Competition Industry Advisory Board for the past 3 years.

Robert holds a Bachelors Degree in Information Technology from American Intercontinental University.

Joe Zacharias, IT Security Specialist, Information Security Professional

Joe is the Computer Security Incident Response Team (CSIRT) Lead for a large Financial Services company in Central Illinois. He has 10 years of IT experience in the Financial Services industry, with concentrations in security risk management, incident response, security architecture consulting, and vulnerability management. Joe holds MCSE and ACSA industry designations. He has an undergraduate degree from Loyola University Chicago, and a masters degree from Northwestern University.