

# Cyber Defense and Disaster Recovery Conference 2014: Distributed Storage Presentations & Speakers - Featured Sessions



## Opening Remarks

Kara McElwrath – Assistant Director of Client Services, IT Services, University of Illinois Springfield

David A. Ford – Special Agent in Charge, Federal Bureau of Investigation

## Keynote Presentation - Cyber Response in the Private Sector - What Should We Be Worrying About?

This presentation will focus on current and future security issues facing the private sector from a "Cyber-Response Perspective". Coming to the realization that we can no longer prevent (Prevention) an attack, we must get much better at detecting (Detection) and remediating (Response). The presenter will discuss the key factors to consider when putting together a Detection and Response Team. These "key factors" include team makeup, tools (traditional and non-traditional), remediation plans, and several others. We will also explore how "moving to the cloud" and Personally Owned Devices (POD) are creating more security challenges for companies both from a response perspective and a risk perspective.

**Todd Wagner, CISSP, Electronic Investigations and Forensics Manager, Caterpillar, Inc.**

## Morning Plenary Session - Finding Information in a Web of Imagery

The world is observed by an enormous collection of cameras --- webcams, satellites and cell-phones. Over the last decade, I have been building tools to characterize, index, and calibrate imagery available on the Internet. I will talk about our success in building 3D models of scene locations, describing how people use public spaces, documenting environmental changes, and, most recently, pinpointing the location of a "lost" grave from photos of the funeral, allowing the St Louis Police department to re-open a 30 year old cold case.

**Robert Pless, PhD, Professor of Computer Science, Washington University**

## Afternoon Plenary Session - Protecting Your Data in the Public Cloud

The shift to cloud computing provides an organization with the ability to focus on its core value proposition and allows for far greater flexibility and capital cost reductions. This shift often changes the way that organizations operate, and presents unique challenges to information security professionals.

The inherent flexibility in cloud computing allows an organization to move data, and applications to a cloud provider. The fact that such an organization no longer houses data and related functions in its own physical structure leads to the concerns about data integrity, data security, and legal requirements. In this talk we will explore what you can do to mitigate your risk for your business as well as what can be done to protect your own personal data.

**Brian Lewis, IT Pro Evangelist, Microsoft Corporation**





### Sensible Approach to BYOD

We are talking about the single greatest evolution that IT is challenged with these days. It is a transformation of not only the device types, but who owns the devices, who manages the devices, who supports the devices. BYOD encompasses smartphones, tablets, as well as any portable device now that has computing power (wrist watches, google glass, etc). And it is not just about the devices, it is also about the software and services that employees want to use -- cloud services and other tools on the web and how we approach the plan to manage them and protect your data.

**Tony Hausmann, Sr. Account Manager, The Newberry Group**

### Digital Forensics: Open Hands-on Lab

Open lab session with hands-on exposure to digital forensics tools. Join us in exploring the deepest recesses of today's systems using forensics tools, such as memory forensic tools. No previous experience required. All levels welcome to attend.

**Frank Fuchs, Certified Forensics Investigator, Instructor, University of Illinois Springfield**

### Remembering the Basics

With today's exploits becoming more and more sophisticated and the specter of compromise becoming more and more real, every once in a while we need to step back and review the basics of security. In this session, William Nicholl of State Farm will facilitate an open discussion of security basics that need to be kept in the forefront of our efforts and implementations. The audience is encouraged to share their views of security basics and how these basics can be put into practice in our varying environments.

**William Nicholl, State Farm Insurance Company**

### Things to Know About the NSA, FISA, and Section 215 that The Guardian (UK) Won't Tell You

Recent reporting over NSA Surveillance has been described as "noise", "more heat than light", and "sensational". Are there better ways of talking about the issues?

Is there a more balanced view that still recognizes Fourth Amendment conflict with compelling government interest, but does not sound like a witch hunt?

We take some time to look at what might be the real issues and what might be productive language to use when discussing the recent "revelations" and the programs they refer to. The issues at stake are certainly important and deserve public attention based on a comprehensive view.

**Ronald P. Loui, PhD, Assistant Professor of Computer Science, University of Illinois Springfield**

### Illusions of Privacy

Understanding the distribution of one's personal information via social networking and open source techniques.

**Stephanie Wright, Special Agent, Cybercrime Investigator, Federal Bureau of Investigation**





**Frank Fuchs, Instructor, University of Illinois Springfield**

Frank Fuchs is a certified computer forensics investigator and an instructor for the University of Illinois Springfield. He currently develops and teaches digital forensic courses at the undergraduate level for the computer science department.

Frank has over 28 years of experience with the Illinois State Police. In 1998, he assisted in the development of an Internet Crimes Against Children Task Force where he worked as a liaison for federal, state, and local law enforcement agencies. He has over fifteen years of experience working as a crime scene and evidence recovery specialist for the Divisions of Internal Investigations and Operations. He has performed hundreds casework examinations and analysis involving digital equipment such as computers, networks, cell phones and video surveillance equipment. Frank was also responsible for overseeing the Criminal Justice Information Systems Triennial Federal Audit before retiring from Agency in 2012.

During his time with the Illinois State Police, Frank has earned several forensic software and investigative certifications which include the EnCase Certified Examiner (EnCE); Computer Forensics Certified Examiner (CFCE); Certified NetWare Engineer (CNE); and Microsoft A+ Certifications

Most recently, in 2013, Frank has joined the faculty of the University of Illinois Springfield where he teaches digital forensic courses. He applies his information technology, investigative and network security experience to help students learn the profession of digital forensics and crime scene techniques.

**Tony Hausmann, Sr. Account Manager, The Newberry Group**

Tony is a Senior Account Manager with The Newberry Group where he specializes in identifying Information Assurance Solutions to solve the Cyber Security challenges faced by large and medium-sized corporations and government agencies. After a lackluster career as an actor, Tony began his IT career in the IT Training Industry in the 1990's and was a regular speaker on the IT Training Conference circuit. Tony joined the Newberry Group in 2007 to provide business development and proposal writing to the firms burgeoning Federal and Commercial Consulting business.

The Newberry Group, Inc. (Newberry) is employee owned and is nationally recognized as a quality IT Services and Cyber Security firm serving government and commercial clients. Headquartered in St. Charles, MO, with an office in Columbia, MD, Newberry provides a full life cycle of services for Information Assurance: Digital Forensics, Data Breach Investigation, Data Loss Prevention, BYOD Security, Vulnerability Assessments, Intrusion Prevention, Web and Email Security, Endpoint and Perimeter Security. Newberry's team of IT support and Information Assurance professionals provide consulting, integration, reseller services and training. [www.thenewberrygroup.com](http://www.thenewberrygroup.com)

**Lance James, Head of Cyber Intelligence, Deloitte**

Author of "Phishing Exposed" and a co-author to "Emerging Threat Analysis", has been heavily involved with the information security community for more than 15 years. With over a decade of experience with programming, network security, digital forensics, malware research, cryptography design & cryptanalysis, attacking protocols and a detailed expertise in information security, Lance has provided consultation to numerous businesses ranging from small start-ups, governments, both national and international, as well as Fortune 500's and America's top financial institutions. He has spent the last few years devising techniques to prevent, track, and detect phishing and malware attacks. He is an advisory board member of the Digital PhishNet (a Microsoft/NCFTA organization) and the Centre for Strategic Cyberspace + Security Science (CSCSS.org), creator of InvisibleNet (IIP/I2P), a prominent member of the local 2600 and InfraGard chapters, and a Co-Founder of Secure Science Corporation. Lance is currently Head of Cyber Intelligence at Deloitte, and is actively engaged with two book projects, "The Threat Intelligence Handbook" (No Starch Press) and "Hacking Back: Offensive Cyber Counterintelligence" (Mcgraw-Hill) slated for Summer 2014.

As a regular speaker at numerous security conferences and being a consistent source of information by various news organizations, Lance James is recognized as a major asset in the information security community.

**Brian Lewis, IT Pro Evangelist, Microsoft Corporation**

Brian Lewis works as an IT Pro Evangelist for Microsoft Corporation in the Midwest, where he focuses on the IT Pro audience in Illinois, Indiana, and Wisconsin. He is very passionate about technology and has over 18 years of enterprise IT experience.

Brian received his Bachelors degree in Management of Information Systems from the University of Wisconsin – Milwaukee. One of Brian's passions is computer security and he holds the Certified Information Systems Security Professional (CISSP) certification among other computer industry certifications.

Brian enjoys working with all computer and networking technologies. He enjoys everything from programming and scripting to working with all types of infrastructure. There just isn't a technology that isn't interesting to him. Brian enjoys several hobbies outside of computers including rock climbing, trail biking, and swimming.





**Ronald P. Loui, PhD, Assistant Professor of Computer Science, University of Illinois Springfield**

Ronald P. Loui, PhD, is an Assistant Professor of Computer Science at the University of Illinois Springfield. He was formerly a tenured professor at Washington University in St. Louis in artificial intelligence and law.

After 9/11, he worked on datamining projects descended from DARPA's TIA, for SAIC, ARDA, IARPA, and DTO in cooperation with the NSA and AFOSR.

He was an original member of the HARVARD INTERNATIONAL REVIEW Military and Technology Section. At the University of Illinois Springfield, he conducts graduate readings seminars in cyberwarfare and in computer surveillance

**Kara McElwrath, Assistant Director of Client Services, Information Technology Services, University of Illinois Springfield**

Kara McElwrath is the Assistant Director of Client Services in the Information Technology Services Department at UIS. She has a rich background in both technology and education, beginning her career as a public school teacher and then moving into corporate training and consulting before coming to UIS in 2007.

**William Nicholl, State Farm Insurance Company**

William Nicholl (Bill) has been working for State Farm out of Bloomington, IL since 2006. Currently, he's the Team Lead for MS Security (Microsoft Security) and Active Directory (AD), both assignments at the Problem Management level. Prior to joining State Farm, Bill worked as a Security Engineer for an Air Force Global Deployment program out of Scott Air Force Base, was a freelance Microsoft Certified Trainer (MCT) specializing in Network Infrastructure, AD design and maintenance, and Security, and worked as a freelance technical writer.

**Robert Pless, PhD, Professor of Computer Science, Washington University**

Robert Pless is a Professor of Computer Science and Engineering at Washington University in St. Louis. His research focus is on data driven approaches to understanding motion and change in video, with a current focus on long term time-lapse imagery. Dr. Pless has a Bachelors Degree in Computer Science from Cornell University and a PhD from the University of Maryland, College Park. He received the NSF CAREER award in 2006, chaired the IEEE Workshop

**Levii J. Smith, Chief Engineer | Solutions Architect, SAIC**

Levii has been consulting and developing technology systems for defense and commercial clients since the mid- 1990's. Now located in the Metro-East St. Louis area he has a global perspective of information handling, having developed the processes and standards for international working groups and agency partners including US Air Force Weather Agency, UK's Met Office, Germany's BGIO, NATO ACOMEX, and the SHAPE data automation groups.

Levi is a 3rd year PhD student specializing in IT & Information Security. He has a Masters of Science in Information Security in and Assurance, and holds a number of industry certifications to include GIAC-G2700, C|DRP, C|EH, C|HFI, and CISSP.

His current focus is the research and application of secure development lifecycles, quantitative management of information security, and the intersection of law, technology, and business as it affects the modern firm. Short works and contact information are available at <http://www.Levii.com>

**Todd Wagner, CISSP, Electronic Investigations and Forensics Manager, Caterpillar, Inc.**

Todd Wagner manages the Caterpillar Computer Security Incident Response Team. Todd is responsible for global cyber response and electronic investigations at Caterpillar. For the last two years, Todd has focused on understanding the Advanced Persistent Threat and the development of Caterpillar's defense against it. He has also served Caterpillar in several other roles including a lead computer security responder, Global Security Investigator and Crisis Coordinator.

Prior to joining Caterpillar in March 2004, Todd served as a Special Agent with the Federal Bureau of Investigation (FBI). While serving the FBI, Todd was responsible for investigating computer related crimes, terrorism, financial and violent crimes. Although involved in all types of investigations, Wagner specialized in Computer Forensics and Terrorism. After 9-11, he took several temporary duty assignments in New Jersey and Washington D.C. These assignments involved conducting computer forensics on computers related to 9-11 and serving as one of several lead agents in a newly formed Terrorism Command Center. Todd was responsible for conducting the computer investigations in Peoria, IL which lead to the conviction of Ali Al-Mari for "Conspiracy to Provide Material Support to a Foreign Terrorist Organization".

Todd is a Certified Information Security Systems Professional. He holds a Bachelor of Arts Degree in Mathematics from Eastern Illinois University and a Master of Education degree from Clemson University.

**Stephanie Wright, Special Agent, Cybercrime Investigator, Federal Bureau of Investigation**

Special Agent Stephanie Wright has worked computer intrusions since she joined the FBI in 2008.

