The 3rd Information Assurance Day

November 9, 2010

Studio 210,Fisher Auditorium – IUP

|  |  |  |
| --- | --- | --- |
| **Time** | **Speaker** | **Topic Title** |
| 9:00 – 9:30 | Dr. Mary Lou Zanich, Interim Dean, College of Natural Science and Mathematics | *Opening Remarks* |
| 9:30 – 10:45 | Mr. Dominic Glavach and Mr. Scott Zimmerman, Concurrent Technologies Corporation | *Cloud Forensics* |
| 10:45 – 11:00 | Break |  |
| 11:00 – 12:15 | Mr. Daniel Larkin, Former FBI Unit Chief Current Director of Strategic Operations - NCFTA | *Recent Evolutions in  the Fight Against  International Organized Cyber  Crime* |
|  | Lunch Break |  |
| 1:45 – 3:00 | Mr. Eric Gruss, Vice President, Reliance Bank, Information Security Officer and the Information Technology Manager | *Network Security, It's More Than Just a Firewall* |
| 3:00 – 3:15 | Break |  |
| 3:15 – 4:30 | Mr.Tom Bianco, District Attorney, Indiana County | *State and Federal Laws pertaining to Cybercrime and prosecution* |

****

For more information, please contact Dr. Rose Shumba (724.357.3166) or Dr. Charles Shubra (724.357.9717).

**Biographical Information**

**Eric Gruss**

Eric Gruss started working with LANs as a systems engineer with LAN Associates in Babylon, N.Y., in 1992. In 1996, he joined Link Computer in Bellwood, PA where he worked with Cisco equipment while supporting NetWare and NT. He then became a Senior Systems Engineer specializing in WANs, VPNs, wireless, and IP telephony technologies. He designed, implemented, and supported large-scale projects across PA and sometimes beyond. In 2003, Eric accepted a position at Reliance Bank, Altoona, PA, where he is now the Assistant Vice President and as well as the Information Security Officer and the Information Technology Manager.

**Tom Bianco**

Tom Bianco took office as the District Attorney of Indiana County in January of 2008.  Tom is a graduate of Penns Manor High School, Indiana University of Pennsylvania, and the Dickinson School of Law.  He has practiced law in Indiana County for over 14 years.  Tom formerly served as the judicial law clerk to the Honorable W. Parker Ruddock and the Honorable William J. Martin.  He also served as an Assistant Public Defender and Assistant District Attorney for Indiana County.

**Dominick (Dom) Glavach**

Dominick (Dom) Glavach, CISSP is an IUP Alumni and Principal Information Systems Security Engineer at Concurrent Technologies Corporation (CTC) with extensive experience in cyber-attack methods, trends, and counter-measures; intrusion detection; computer incident response; and malware analysis. His work at CTC includes numerous Information Assurance projects for CTC and CTC customers. He has designed and implemented Internet exchange point Intrusion Detection Systems; served as a network attack subject matter expert for the National Defense University; developed and coordinated Cyber-exercises for CTC customers; and presented “\*nix Computer Forensics” for the International High Technology Crime Investigation Association.

Concurrent Technologies Corporation (CTC) is an independent, nonprofit, applied scientific research and development professional services organization providing innovative management and technology-based solutions to government and industry. Established in 1987, CTC operates from more than 50 locations with a staff of over 1,400 employees. As a nonprofit 501(c)(3) organization, CTC’s primary purpose and programs are to undertake applied scientific research and development activities that serve the public interest. We conduct impartial, in-depth assessments and technical evaluations that emphasize increased quality, enhanced effectiveness, and rapid technology transition and deployment. CTC offers a broad range of services and capabilities, coupled with real-world experience.

**Daniel Larkin**

Mr. Larkin established the first Cyber Fusion Unit for the Federal Government, enabling Govt/Law Enforcement to effectively co-locate with Subject Matter Experts (SMEs) from industry & academia, substantially enhancing resource sharing (personnel, technology & intelligence) to the mutual benefit of all participants.  This unique collaborative effort also has helped build crucial cross-sector trusted relationships, as a vital foundation of this alliance.   This multi-faceted fusion team continues to develop unprecedented intelligence and resource capabilities for the participants, and is viewed as a model for developing additional (franchise) public/private alliances across the U.S and in a growing number of countries worldwide.  Private Sector partners include numerous financial services organizations, telecommunications, technology, e-commerce and several NSA certified Academic Institutions of Excellence.  Law Enforcement partners include a growing list of Federal, State & Local agencies, as well as international investigators from more than a dozen countries.

As the FBI Unit chief of the Internet Crime Complaint Center (IC3) Mr. Larkin expanded the focus of this project to include hundreds of SMEs from industry & academia as major contributors of both intelligence and exceptional analytical skills.   He also oversaw the major overhaul of the IC3 complaint management system, and directed the development and successful completion of numerous international cyber crime initiatives, in which more than 500 arrests and millions of dollars in seizures were accomplished.

Prior to that Mr. Larkin was a Supervisory Special Agent (SSA) for ten years, where he oversaw numerous regional and national joint agency initiatives,  involving public corruption and fraud associated with many federal, state, and local agencies.  He also served as Team Leader in the “Operation Illwind” Pentagon scandal, contract fraud & corruption investigation, which led to record settlements and convictions in the late 1980’s.

Mr. Larkin also developed one of the first High Tech Crime Task Forces in the United States incorporating SME resources from multiple sectors, including federal, state & local government married with high technology, financial services, telecommunications and academia from the private sector.   This unique collaboration of assets included partnerships with the Computer Emergency Response Team (CERT/CC) at Carnegie Mellon University, and led to the development of the first national Public/Private Alliance to identify and combat cyber crime, known as the National Cyber Forensics & Training Alliance (NCFTA).

**Additional Accomplishments**

* Authored the FBI's National Cyber Crime Strategy
* Established first Public/Private Alliance Joint (Industry, Academia & law enforcement) initiatives for the FBI addressing Criminal Spam, Phishing-Credit Card Fraud, Identity Theft and International Money Laundering, which are continuing.
* Initiated and managed first FBI National Undercover Operation, targeting international Cyber Crime.
* Oversaw numerous Joint L.E Initiatives in which more than 500 individuals and organizations were prosecuted domestically and abroad.
* Established first L,E resource sharing & education initiative between FBI & West Africa (Nigeria & Ghana)
* Developed the Internet Risk & Resource Assessment Project (IRRAP) to educate and empower law enforcement and secondary educators regarding child exploitation via the Internet.
* Honored as Distinguished Alumni in 2008 from Indiana University of Pennsylvania.

**Scott Zimmerman**

Mr. Zimmerman has 27 years of IT and Cyber Security experience and is a Principal Technical Advisor at Concurrent Technologies Corporation in Johnstown, PA. Mr. Zimmerman’s education includes a BS in Management Information Systems and AS in Electronic/Computer Technology. He is a Certified Information Systems Security Professional (CISSP); Information Systems Security Engineering Professional (ISSEP) and a member of the Cloud Security Alliance. Mr. Zimmerman has gained a broad background in Information Technology and Information Assurance/Security including: Network Operating Systems; Information Assurance Systems; Forensics; Network Management Systems and Network Modeling and Simulation tools.  In addition to his technical skills he has 16 years of program management experience.  He currently serves as a Technical Director on several DoD/IC programs. This session will address a variety of technical issues concerning cyber forensics in the cloud as well as provide an overview of what cloud computing is.

**Abstracts**

**Dominic Glavach and Scott Zimmerman**

According to research firm Gartner, cloud computing services revenue should total $56.3 billion for 2009, representing a 21.3% increase compared to 2008. The market is expected to explode to $150.1 billion in 2013 (1).  This trend toward cloud computing is creating numerous challenges for cyber forensics professionals.  In traditional models, an Information Assurance or digital forensics professional operated in a domain where system components where within physical reach and ownership boundaries were well defined. The forensic analyst worked directly for an organization and had access to- if not directly administered – the organization’s computing infrastructure.  An organization’s network infrastructure had uniform configurations and settings, that they could collect, preserve or analyze. For example, date stamps were consistently applied, and memory allocation and overwrite procedures were clearly and evenly executed. These consistent system configurations and behaviors (or breaches of anticipated behaviors) were an integral component of a forensic investigation. In a cloud model, consistently configured network infrastructure become less consistent.  For example, because user systems and cloud systems can be separately administered, date stamp settings may differ from the user side and the provider side where the requested application lives in a cloud.  How then to match up a user request and actual use time?

**Eric Gruss**

Practical methods of assessing and mitigating risk through a multilayered approach to security will be presented; proper firewall rules, VLAN use, server ports and services, user access rights and desktop security.

**Tom Bianco**

The DA will present the State and Federal Laws pertaining to Cybercrime and prosecution, and laws governing digital evidence and concerns related to applicable Federal statutes (such as the Electronic Communications Privacy Act of 1986 (ECPA) and the Cable Communications Policy Act (CCPA), both as amended by the USA PATRIOT ACT of 2001, and/or the PrivacyProtection Act of 1980 (PPA)), State statutes, and local policies and laws.

