The 4th Annual Information Assurance Day
November 10, 2011
Delaware Room – HUB – IUP

Time Slot	Speaker	Topic Title
8:40 – 9:00	Dr. Deanne Snavely, Dean College of Natural Science and Mathematics	*Opening Remarks*
9:00– 9:45	Mr. David C. Brown - Business CyberSecurity, Inc.	*Four Essential Requirements for Securing Your Enterprise*
9:45 – 10:45	Mr. Greg Porter - Allegheny Digital and Mr. Matthew Stewart - Robert Morris University	*Making sense of the security data generated by multiple devices* *Using open community software to identify network based security risks to sensitive Information*
10:45- 11:00	Break	
11:00-12:00	Mr. Mark Yanalitis – Highmark, Pittsburgh	*Red Teaming approaches, rationales, engagement risks, and methodologies*
12:00-1:00	Lunch Break	
1:00-2:00	Special Agent Jason Pearson and Special Agent Keith Mularski - Pittsburgh Division of the Federal Bureau of Investigation (FBI)	*What keeps me up at night?*
2:00-3:00	Mr. Harley Parkes - NSA	*TBA*
3:00-4:00	Mr. Douglas Brown - First Commonwealth Bank, Indiana	*Information Assurance, an IT Audit Perspective*

For more information, please contact Dr. Rose Shumba, Director, Institute of IA Education, shumba@iup.edu,724.357.3166

BIOGRAPHICAL INFORMATION

DAVID C. BROWN

David C. Brown, CISSP, PMP, CEH, is the president and founder of Business CyberSecurity, Inc., www.BusiessCyberSecurity.com. He is also the inventor of its innovative business information framework model and analysis methodologies. He has more than thirty years of experience in information technology and analysis of business processes combined with more than twenty years of addressing information security issues. He has held a wide variety of engineering, consulting, and management positions in small and large companies.

He holds a Six Sigma Green Belt and ITIL Foundations certification, has earned a Bachelor of Science in management information systems, a certificate in Computer Forensic Technology, and an Associate's Degree in Electronics and Computer Technology.

GREG PORTER

Greg Porter is the founder of Allegheny Digital, a Western Pennsylvania based information security company specializing in network infrastructure security, incident response, enterprise risk management and managed security services. For the past several years, Mr. Porter has both led and delivered comprehensive assessment activities that monitor, test and audit the effectiveness of information system security, risk managed governance and controls, and regulatory conformance. He holds a Bachelor of Science degree in Chemistry from the University of Pittsburgh, a Master of Science degree in Information Technology (Information Security Concentration) from Carnegie Mellon University and a Master of Science degree in Health Care Policy and Management (Highest Distinction) also from CMU. In addition, Mr. Porter maintains several information security related certifications and is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM).

MATTHEW STEWART

Matthew Stewart is the Director of Information Security at Robert Morris University. In addition, he is an adjunct professor teaching Computer Security, Intrusion Detection, and Computer Forensics.

Matthew earned his Master's Degree in Information Security and Assurance and also holds undergraduate degrees in Information Systems Security and Computer Forensics. He holds several leading industry certifications including the Certified Information Systems Security Professional (CISSP), SANS GIAC Certified Intrusion Analyst (GCIA), and the SANS GIAC Certified Incident Handler (GCIH). He is a member of SANS Advisory Board and is a local SANS Mentor in Pittsburgh.

MARK YANALITIS

Mr. Yanalitis has held positions in the private and public sector as a network security engineer, a Big-4 accounting firm security consultant, and Director of Security for a large regional ISP/MSP. He currently functions as an Enterprise Technical Consultant fulfilling the role of IT Infrastructure Architect for a national health insurance concern. His efforts have concentrated upon enterprise security architectures, threat management, Intelligence life cycle management, and incident response.

Mr. Yanalitis has presented material at INFOWARCON, ISSA, CMU/SEI SOA workshop, DOJ/FBI Quantico, and ISACA. Past committee membership include National Cyber-Forensics Training Alliance - a joint public-private forensic computing cooperative based in Pittsburgh; the NIST/URAC Healthcare Security Workgroup, and former “At-Large” member of the Board of Directors Pittsburgh Infragard. Presently, he is a committee member on the FS-ISAC Portal Product Selection workgroup and public relations point of contact for the newly formed Pittsburgh Chapter of Open Web Application Security Project (OWASP). He is the founder of the LinkedIn Open Source Intelligence Professionals Group – an international professional group dedicated to open source intelligence methods and tradecraft.

Mr. Yanalitis is a member in good standing with the Association for Computing Machinery (ACM), Armed Forces Communications Electronics Association (AFCEA), and Federation of American Scientists (FAS). He holds CISSP designation and IAM recognition by the Information Security Assurance Training and Rating Program (ISATRP). He has held various vendor technical certifications. Mr. Yanalitis is a graduate of the 8th Pittsburgh FBI Civilian Academy program, and the Duquesne University Wecht Forensics Science and Law program. He holds graduate degrees from the University of Pittsburgh and American Military University.

SPECIAL AGENT JASON PEARSON

Jason Pearson is a Special Agent assigned to the Pittsburgh Division of the Federal Bureau of Investigation (FBI). Prior to joining the FBI, Mr. Pearson formed an Information Technology firm out of Chicago, Illinois. As proprietor of the company, Mr. Pearson led a variety of IT security investigations, and worked as a network/systems engineer. In 2009, Mr. Pearson joined the FBI and was assigned to the Bureau's Cyber Squad and High Tech Crimes Task Force where he currently investigates both National Security and Criminal Cyber Crime offenses.

Mr. Pearson is currently on the front line of investigations involving some of the largest and most complex financial fraud schemes to date and has assisted on a number of investigations involving Counter Intelligence and Domestic Terrorism matters. Mr. Pearson's expertise involves sophisticated Botnets and Malware, Computer Intrusion matters, and Automated Clearing House (SACH) fraud.

SPECIAL AGENT KEITH MULARSKI

Keith Mularski is a Supervisory Special Agent assigned to the Pittsburgh Division of the Federal Bureau of Investigation (FBI). Mr. Mularski received his appointment to the position of Special Agent with the FBI in 1998. After attending the FBI Academy in Quantico, Virginia, Mr. Mularski was assigned to the FBI's Washington Field Office where he investigated National Security Matters for seven years. During this time Mr. Mularski worked on a number of high profile investigations such as the Robert Hanssen espionage investigation and the 9/11 Terrorist attack on the Pentagon.

In 2005, Mr. Mularski transferred to the FBI's Cyber Division and was detailed to the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania. While detailed to the NCFTA, Mr. Mularski successfully worked with Private Industry Subject Matter Experts on a number of joint Cyber-Crime initiatives with an emphasis in the development of proactive targeting of organized international Cyber-Crime groups. From 2006 through 2008, Mr. Mularski worked undercover penetrating cyber underground groups which resulted in the dismantlement of the Darkmarket criminal carding forum in October 2008. In 2010 Mr. Mularski received the FBI Director's Award for Excellence in Outstanding Cyber Investigation.

In 2011, Mr. Mularski transferred to the FBI's Pittsburgh Field Office. Mr. Mularski is currently the supervisor of the Cyber Squad which responsible for all Cyber investigations in Western Pennsylvania and West Virginia.

HARLEY E. PARKES

Chief, Mission & Technical Vulnerability Office
National Security Agency/Central Security Service

CURRENT POSITION: Mr. Parkes, a member of the Defense Intelligence Senior Executive Service, is the Chief of the Mission and Technical Vulnerability (MTV) office in the Information Assurance Directorate (IAD) of the National Security Agency. The MTV organization conducts Communications Security (COMSEC) monitoring and Technical Security Evaluations to evaluate the overall security of U.S. Government communications and operations. As MTV Chief, he also serves as the Director of the Joint COMSEC Monitoring Activity (JCMA) which operates an enterprise of monitoring centers located throughout the world.

EDUCATION: Mr. Parkes holds a Bachelor of Science degree in Computer Science from the University of Maryland.

PRIOR POSITIONS: Mr. Parkes has worked in the cryptologic career field for 30 years. He started his career in the U.S. Air Force as a collection officer. In January 1983 he was hired by NSA and served in a number of technical and supervisory positions within the Directorate of Operations between 1983 and 1995. In June 1995, he was assigned to NSA/CSS Pacific and spent four years providing cryptologic support to USCINCPAC and PACOM's service components. In 1997 he established, and became the first ever lead of, the Computer Network Vulnerability Team at NCPAC. This team provides computer network security consultations in support of USCINCPAC and its components. In 1999 he returned to NSA Headquarters to continue this work within the Vulnerability Analysis and Operations group of IAD. He became D/Chief of the Operational Network Vulnerabilities (ONV) office in October 2008. The ONV works to strengthen DoD and the national security communities' operational networks through vulnerability assessments, in-depth technical analysis, and long-term integrated best-practice community security solutions. In 2010, Mr. Parkes became Chief of the MTV.

PROFESSIONAL BACKGROUND: He serves as the NSA representative to the Enterprise Solutions Steering Group (ESSG) and is a member of the Technical Advisory Board for the Tower Federal Credit Union

PERSONAL: Mr. Parkes was born in Washington, PA. He resides in Harford County, Maryland with his wife Michelle and their two children, Tyler and Kaylee. He enjoys softball, football and coaching his son's little league baseball team.

DOUGLAS BROWN

Doug graduated from IUP in 1981 with a major in MIS and minors in Economics and Accounting. Since that time he has worked for several financial institutions in several states all in the field of Information Technology Auditing. He started his career as an audit programmer analyst where he worked closely with operational and external auditors learning the audit profession. He created unique audit tests to verify data integrity. He ascertained from his tests that company information had a personality quality to it that permitted a unique view of a company especially in regards to how effective and efficient a company operated. He also was able to expose frauds, errors, misuse of system features, and reveal improperly designed application systems. Doug has also conducted numerous audits of technology systems, applications, production processes, regulatory and compliance directives, product and system life cycles, and service providers. Doug has assisted IT, Executive Management, and the Board of Directors in developing Risk Management and Governance practices. Doug currently is the Senior Vice President and IT Audit Senior Manager for First Commonwealth Financial Corporation located here in Indiana, Pennsylvania.

ABSTRACTS

DAVID C. BROWN
Topic: Four Essential Requirements for Securing Your Enterprise
Abstract:
What makes cybersecurity so difficult for the defenders? If the government, with all of its resources repeatedly gets hacked, what can you do to defend your enterprise? We will show you a new approach to cybersecurity that will change your perspective and help your organization to build better defenses.

MATTHEW STEWART (Matt) and GREG PORTER (Greg)
Topic: Making sense of the security data generated by multiple devices
Abstract (Matt)
In this talk we will discuss how to make sense of all of the security data generated by multiple devices. We can gain a clear picture of meaningful attacks and how to mitigate them through the aggregation and correlation of data collected from key points on the network including firewalls, intrusion detection systems, hosts and vulnerability assessment solutions.

Abstract (Greg)
Topic: Using open community software to identify network based security risks to sensitive Information
Abstract:
The theft of sensitive information continues to challenge both the public and private sector alike. Adequate network situational awareness can provide the difference between detecting a hacking/IT incident or potentially ending up as a statistic on the Dataloss db website. This presentation will provide key considerations for using open community software to identify network based security risks to sensitive information.

MARK YANALITIS
Topic: Red Teaming approaches, rationales, engagement risks, and methodologies
Abstract
The presentation discusses Red Teaming approaches, rationales, engagement risks, and methodologies. “Low-and-slow” traditional open-sources intelligence collection and tradecraft techniques are force-multipliers in successful exams. In the rush to get on the target, engagement preparation and thorough reconnaissance often become abbreviated. Missed intelligence often leads to prolonged engagement timelines, susceptibility to cognitive biases, missed opportunities, attack deceleration, and an over-reliance on automated tooling logic.

SPECIAL AGENT JASON PEARSON and SPECIAL AGENT KEITH MULARSKI
Topic: "What keeps me up at night..."
Abstract
A discussion of Botnets, Malware, Cyber Crime & the Criminal Underground

DOUGLAS BROWN
Topic: Information Assurance, an IT Audit Perspective.
Abstract:
Auditing as it relates to information assurance.