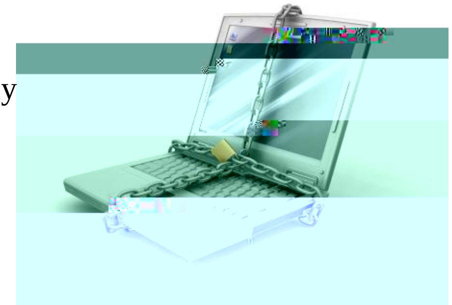
The 4th Annual Information Assurance Day
November 10, 2011
Delaware Room – HUB – IUP



Time Slot	Speaker	Topic Title
8:40 – 9:00		

MATTHEW STEWART

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 t(in)-8Tm5Cr C5.

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

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

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.