ISACA
Serving IT Governance Professionals

San Francisco – 2010 ISACA Fall Conference
Speaker Information

You Have Been Hacked, But Where's the Evidence? A Quick Intro to Digital Forensics

Bill Pankey, Tunitas Group

Professional Strategies Track – Session S23

Abstract:

Often, the first indication of a security breach comes from external sources such as bankcard processors, partners, consumers, or regulators. Almost equally as common is the finding of 'no evidence' in systems to account for the breach or misuse of data. Unfortunately, such negative findings are more a statement about the competence of the investigator that the actual state of the system. This talk provides a rudimentary introduction into computer forensics identifying the basic issues, strategy and tools to identify, recover and preserve the digital evidence of security breaches. The talk is directed at security professionals, incident handlers and auditors of an organization's incident handling procedures.

At the conclusion of the talk, attendees will be able to acquire, preserve and analyze basic evidence in a forensically appropriate way. Examples from the forensic analysis of compromised Windows and Linux systems will be used to demonstrate tool use and key points. Handouts to attendees will include, on DVD, a forensic toolkit.

Target Audience:

Skill level : Beginner; Intermediate
Occupation: Incident handlers, Audit, Security
Occupational Experience: operational

COBIT Objectives:

Speaker Bio:

Bill Pankey is a IT risk professional focused in the health sector. He is a GIAC Certified Incident Handler, a GIAC Certified Forensics Analyst as well as a CISSP, CISA, CGEIT. He is a SANS Institute Mentor for SANS 504 (Incident Handling & Advanced Hacking) and SANS 508 (Computer Forensics). He was the Chapter's CGEIT coordinator for the 2009-2010 cycle and over 400 candidates worldwide availed themselves to his online CGEIT Exam Prep course.