Are You Insecure About Cybersecurity?
November 17, 2015

Agenda

Panel 1: The Cyber Threat Landscape: What You Don’t Know Can Hurt You
- Current faces of cybercrime
- Common causes of data loss – internal and external
- Consequences of a data security/privacy breach
- Regulatory scrutiny of data security standards
- Liability exposure and the legal landscape
- Supply chain risks
- How data breach squares with most insurance coverage

Panel 2: Compliance and Preparedness: Best Practices for Minimizing the Likelihood and Severity of a Data Security Incident
- Cybersecurity best practices, policies and protocols
- Data security/privacy guidance and the NIST framework
- Protecting the perimeter vs. the “crown jewels”
- Incident response planning
- Meeting data security/privacy compliance obligations
- How indemnification and cyber-insurance can manage risk
- Employee awareness and training
- Security audits and penetration testing
- Data breach table top exercises

Panel 3: Into the Breach: Responding to and Remediating a Data Security Incident
- Incident response measures
- Internal investigation
- Forensic investigation
- Law enforcement investigation
- Notification obligations
- Communication plans
- International implications
Meet Our Speakers

**Special Agent AJ Nazario**
Head of Miami Electronic Crimes Task Force (MECTF)
U.S. Secret Service

AJ Nazario began his career with the United States Secret Service (USSS) in April 1992 in the Baltimore Field Office. During his twenty-three year career with the USSS, he has also been assigned to the Vice Presidential Protective Division and the USSS James J. Rowley Training Center. In July 2005, he was reassigned to the Miami Field Office (MIA) where he currently serves as the Assistant to the Special Agent in Charge (ATSAIC) supervising the Miami Electronic Crimes Task Force (MECTF).

**Aurora Fagan**
Assistant U.S. Attorney, Computer Hacking and Intellectual Property (CHIP) Unit
U.S. Attorney’s Office, Southern District of Florida

Aurora Fagan has been an Assistant United States Attorney in the Southern District of Florida since 2007. She is currently one of two attorneys in the SDFL assigned to the Computer Hacking and Intellectual Property (CHIP) Unit, where she handles federal cases involving network intrusions, computer fraud, and intellectual property crimes. She also handles financial crimes, including money laundering, foreign bribery, tax fraud, and bank fraud. Aurora is the District’s point of contact for all national security cyber matters. Prior to joining the USAO, Aurora served as supervising deputy attorney general with the Computer Analysis and Technology Unit at the Division of Criminal Justice in New Jersey. She prosecuted various computer related crimes, including crimes against children, child pornography, network intrusions, identity theft, and denial of service attacks, and led a statewide computer crime task force comprised of prosecutors, civilian investigators and various law enforcement officers from around the state. Aurora also served as assistant district attorney in New York City, where she prosecuted narcotics cases, financial crimes and computer crimes. She has given various lectures on searching and seizing digital evidence, legal issues and ethics in a high tech world, and other computer crime related topics for national organizations such as the NDAA, APRI, HTCIA, and RCFG.

**Supervisory Special Agent Jason Manar**
Miami Division-Cyber Crime
FBI

As the Supervisory Special Agent for Miami Cyber Crime, Jason Manar manages all criminal cyber operations within the Southern District of Florida. Prior to his current role he served at Headquarters in the Major Cyber Crimes Unit combating cyber criminal threats targeting U.S. entities. Previously, he has served as the Safe Streets Gang/Violent Crime Task Force Coordinator for the FBI’s Springfield Division and worked high level public corruption and health care fraud cases in the Detroit Division. All these experiences have yielded an invaluable holistic cyber crime perspective. Prior to joining the FBI, he served approximately six years with the Kentucky State Police as a Trooper and Detective.
Keith Lowry
Senior Vice President, Business Threat Intelligence and Analysis
Nuix
Keith has more than 25 years of experience implementing, managing, and directing insider threat, counterintelligence, and intelligence collection programs. Prior to joining Nuix, Keith served as the security liaison officer for the U.S. Food and Drug Administration, where he lead the FDA's counterintelligence and insider threat program activities. Keith is the former chief of staff to the deputy under the secretary of defense for Human Intelligence, Counterintelligence and Security at the Pentagon. He also served as the chief of strategy and evaluation for the director of National Intelligence. In this capacity, Keith oversaw a team to develop and publish the U.S. National Counterintelligence Strategy, and implemented policies in the areas of counterintelligence, counterterrorism, counterproliferation, insider threats, and technology enablers. He is a former law enforcement officer and High-Technology Crime Unit detective with the City of San Jose California, where he investigated unauthorized computer access, computer and component theft, trade secret and intellectual property theft, employee theft, and cellular phone fraud. He was cross-sworn as a U.S. Federal Marshall and participated in multijurisdictional investigation teams involving international organized crime groups.

Ronald E. Plesco, Jr., Esq.
Principal and National Lead, Cyber Investigations
KPMG
Ron is an internationally known information security and privacy lawyer with 16 years of experience in cyber investigations, information assurance, privacy, identity management, computer crime, emerging cyber threats, and technology solutions. Ron is the national lead of KPMG's Cyber Investigations, Intelligence and Analytics practice. Prior to joining KPMG, Ron was the CEO of the National Cyber Forensics and Training Alliance (NCFTA), where he managed the development of intelligence that led to over 400 worldwide cyber crime arrests in four years, and prevented over $2 billion in fraud. Notable NCFTA intelligence-led arrests include Ghost Click, Anonymous, Coreflood and multiple online frauds.

Ted Sullivan
Senior Vice President, Sales and Breach Services
Equifax Personal Solutions
Ted leads business development for Equifax's Personal Solutions breach and partner business. When an organization experiences a large breach Ted provides remediation services for the affected individuals, using the details of the breach, including the type information that was compromised, how it was lost, and the number of affected individuals to best match the services offered to the risk of the data lost. Equifax provides notification and call center services in addition to a suite of breach products that include credit monitoring, identity protection, identity theft insurance, and restoration assistance.
Meet Our Moderators

Jeffrey C. Sharer
Co-Chair, Data Law Practice
Akerman LLP

Jeffrey's practice encompasses information governance, e-discovery, and privacy and data protection. Jeffrey advises and advocates for clients at all stages of the discovery lifecycle, from preservation through production, in litigation and regulatory matters, and internal and governmental investigations. Jeffrey has significant experience with design, implementation, negotiation, and litigation of e-discovery best practices. He is at the forefront of using predictive coding and other analytic technologies in discovery to help clients save time and costs, and improve defensibility of process. Jeffrey helps clients mitigate risk, reduce cost, and create business value outside the dispute context through sound, end-to-end governance of enterprise data. He advises clients on the development and implementation of records retention policies and schedules, litigation preparedness and discovery strategy, defensible disposition of email and other electronic and hard copy information, and “e-policies” such as “bring your own device,” social media, information classification, and data privacy.

Martin T. Tully
Co-Chair, Data Law Practice
Akerman LLP

Martin is nationally recognized for his experience in the field of electronic discovery and information governance. In these areas, he helps clients stay ahead of the curve with respect to developing law, technology, and best practices concerning e-discovery in both litigation and regulatory matters. Martin has written and presented extensively on e-discovery, digital evidence, information governance and legal technology. He is a veteran trial lawyer with national experience representing companies and individuals in complex commercial litigation concerning a broad array of fields and industries. Martin routinely represents clients in cases involving contract disputes, business torts, defamation, antitrust claims, trade secrets, and consumer class action defense.

Elizabeth F. Hodge
Of Counsel, Healthcare Practice Group
Akerman LLP

Betsy represents a variety of healthcare providers in compliance and transactional matters. Betsy provides guidance to clients, including physicians and hospitals, regarding compliance with applicable federal and state statutes and regulations. These include the HIPAA regulations, state laws regarding physician self-referrals and patient-brokering, and laws concerning human research. Betsy has developed significant experience regarding Security, Data Breach Notification, the HIPAA Privacy, and Administrative Simplification regulations. Betsy also assists clients in buying and selling their healthcare businesses.