CYBER FRAUD & DATA BREACHES
16 CPE's
May 16-17, 2018

Cyber fraud attacks happen; they can't all be stopped. The higher order question must be how can we, as fraud examiners and assurance professionals, best assist our clients in building control defenses that are much more resilient to continual attack? We need to be able to respond at scale to the challenges we face from a fully automated criminal hacker community. Time and time again, we've seen those with ill intent automate their increasingly more complex attacks; it's this ability that has led to a paradigm shift in cyber fraud, moving from a one-on-one to a one-to-many affair.

Losing data to fraud can be costlier than the loss of cash and other assets. To ensure data security, safeguard intellectual property and guard against cyberfraud, fraud examiners must stay informed about rapidly advancing technologies, emerging business trends and the methods employed by increasingly sophisticated information thieves.

This 2-day, instructor-led course will clarify these issues while guiding you through the crucial strategies needed to mitigate the threat of malicious data theft and minimize the risk of inadvertent data loss. You will also learn useful steps for the creation of data security policies and related internal controls.

You Will Learn How To:

--Explain the ways data can be stolen by employees and information thieves;
--Enact data security measures and be prepared in the event of a data breach;
--Contend with data theft maneuvers such as social engineering, hacking and espionage;--Identify various sources of data loss, both internal and external;
--Recognize the impacts of converging trends such as cloud computing and bring your own device (BYOD);
--Recognize the legal and regulatory concerns related to data security.

Who Should Attend:

Certified Fraud Examiners and other anti-fraud professionals
Governance, risk management and compliance officers
Corporate managers
IT professionals
Loss prevention and security professionals
Government employees
Internal and external auditors, CPAs, CISAs, and CAs
Business professionals, educators and students interested in the fraud prevention field

	DAY ONE	DAY TWO
7:30 a.m. - 8:00 a.m.	***Registration & Continental Breakfast***	***Continental Breakfast***
8:00 a.m. - 9:20 a.m.	**Introduction to Data Protection and Information Security** In this opening session, you will learn what intellectual property is; the types of information that are susceptible to loss, theft or misappropriation; common causes of data breaches; the types of individuals who perpetrate information theft; common motivations driving information theft; types of threats to proprietary information; common challenges with protecting information assets; and possible repercussions of data breaches.	**Risks of Social Media in the Workplace** The use of social media provides many benefits to organizations, but it also creates numerous risks. This session examines the role of social media in today's business environment, focusing on the problems that can occur when using social media and the measures that organizations can take to reduce such risks.
9:20 a.m. - 9:35 a.m.	***Break***	***Break***
9:35 a.m. - 10:55 a.m.	**Legal Issues in Information Security** Every country has laws and regulations that concern information security. This session examines some of the key legal issues concerning the protection of data and intellectual property.	**Managing the Risks of Bring Your Own Device Programs** Bring your own device (BYOD) refers to the concept whereby employees bring their own personal electronic devices to work and use them to work. Embracing BYOD offers several advantages to organizations, but it also creates challenges and risks. This session examines those advantages and risks and it discusses ways organizations

		can minimize risks associated with BYOD systems.
10:55 a.m. - 11:10 a.m.	***Break***	***Break***
11:10 a.m. - 12:30 p.m.	**Corporate Espionage 101** Corporate espionage, which refers to the use of illegal means to gather information for commercial purposes, is a major issue for the business world. This session examines corporate espionage, focusing on targets of corporate espionage, industries that make attractive targets for corporate espionage, various forms of corporate espionage, different ways to move data, insider threats, and case studies that highlight the motivations and methods behind theses schemes	**Cloud Computing** Organizations and individuals are increasingly storing data and applications on the cloud, but there are risks associated with using cloud-based infrastructure. This session examines cloud computing, focusing on the characteristics and models of cloud computing, compliance issues that arise in the cloud, security challenges with the cloud, and the protection of data in the cloud.
12:30 p.m. - 1:30 p.m.	***Lunch On Your Own***	***Lunch on Your Own***
1:30 p.m. - 2:50 p.m.	**Corporate Espionage: Where Attackers Get Information** This session will explore the variety of techniques that fraudsters employ to obtain trade secrets, proprietary information and information that they can use to develop knowledge-based attacks.	**Responding to Data Breaches** To help ensure that an organization responds to data breaches timely and efficiently, management should have an incident response plan in place that outlines how to respond to such issues. This session explores the basic elements of incident response plans.
2:50 p.m. - 3:05 p.m.	***Break***	***Break***
3:05 p.m. - 4:25 p.m.	**Social Engineering** This session will cover the means by which attackers use social engineering tactics to gain access to targets' information resources. It will focus on why social engineering attacks succeed, the different categories of social engineers, the types of information that social engineers target, common red flags of social engineering schemes and measures to prevent becoming a victim of social engineering attacks.	**Data Breach Prevention** To prevent the loss or misuse of data or proprietary information, organizations should develop and implement risk-based information security systems designed to detect and prevent unauthorized access to sensitive information. This session examines the key components to an effective information security system.

CARY E. MOORE, CFE, CISSP, MBA

IBM Red Cell Team Leader, Associate Partner
Global Banking Counter Fraud & Financial Crimes

With a career distinguished by 14 years of highly decorated service to the United States Air Force, of which seven were as a Federal Agent for the Air Force Office of Special Investigations (AFOSI), Mr. Moore has more than 17 years of specialized experience in cybersecurity, enterprise forensics, and technical surveillance countermeasures (TSCM). Focusing on counterintelligence and counterespionage, he brings a unique perspective to insider threats and protecting some of the nation's most sensitive data.

During his time with AFOSI, Special Agent Moore participated in investigations on a global scale, where he quickly gained notoriety with covert remote forensics as a new technique in the industry. These techniques brought new capabilities to investigations by allowing evidence to be captured and analyzed in real-time without compromising or disclosing the investigation.

Special Agent Moore was one of the first Computer Crime Investigator Agents sent to the TSCM school, hosted by the National Security Agency. Looking for innovative ways to detect compromised computers exploited as surveillance devices, he designed a tool to quickly identify areas of possible compromise. This tool was incorporated into the curriculum and circulated to agents around the world as an effective way to identify compromised systems. This training also gave him specialized experience in physical security, radio frequency analysis, and audio and video penetration detection.

Following his years with AFOSI, Mr. Moore joined Guidance Software, the makers of EnCase Computer Forensic and eDiscovery software. Supporting clients around the world, he conducted incident response and e-discovery engagements. After promotion to Technical Director (cybersecurity), he worked with federal public-sector clients for incident response. Prior to his current role, he served as a Senior Vice President, Cyber Intelligence and Emerging Threats Manager at Bank of America. Finding innovative ways to "rob a bank" and banking customers, he devised controls to prevent the fraud from ever being realized. Currently, he is an Associate Partner for the IBM Red Cell Team where he conducts dark Web intelligence gathering, operations to identify compromised accounts, and ways to get in front of fraud. He also serves as an Adjunct Faculty Instructor for the Association of Certified Fraud Examiners.

Mr. Moore is an accomplished speaker who has lectured in national and international forums, including US-CERT GFirst Conference, DoD Cyber Crime Conferences, and as a Technical Keynote Address delegate to the 2009 NATO IA Symposium. As an authority in evidence

seizure, data recovery, and computer forensics, his expert testimony has been crucial in multiple court cases.

In addition to his professional experience, Mr. Moore holds well-respected industry certifications, including Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE), and (formerly) the EnCase Certified Examiner (EnCE) certification. He is a member of the High Technology Crime Investigation Association, the Information Systems Security Association, and a founding member of the International Information Systems Security Certification Consortium, Houston Chapter. He earned a bachelor's degree in Information Technology and a master's degree in Business Administration.