Thursday, May 5, 2022

8 a.m. to 2 p.m. ET

Hershey Country Club, Hershey

Agenda

8 a.m. **Registration and Continental Breakfast — Exhibits Open**

8:30 a.m. **Welcome and Opening Comments**
– *Adam Friscia, Membership and Events Executive, PA Chamber*

8:35 a.m. **How to Do a Forensic Investigation of an Insider Threat**
– *Kate Davenport, Director of Digital Forensic Division, Information Network Associates, Inc. (INA)*
Businesses are under siege with continuous, frequent security attacks, and many of these come from inside. With hybrid now the way most companies have employees working, there are even more opportunities for the "bad apple" employee to do damage. You suspect an insider threat, what should you do as part of your forensic investigation? We will discuss:
- As the IT professional you find disturbing information that may show an employee is sabotaging the data systems. What are the first steps you should take to immediately protect the company? How should you notify HR, the CFO and the President?
- When do you step back and let HR and the CFO handle this?
- How do you protect the evidence?
- The forensics you follow may be needed in a court hearing. What are the forensic steps to uncover all sabotage, and what are the general protocols you need to follow that HR may need?
- What steps should you put in place to ensure no other employee can cause the same type of potential damage?

9:30 a.m. **Staying Ahead of Ever-Changing Security Compliance Standards**
– *Michael T. McAllister, CPA, Partner and Leader of IS Assurance and Advisory Services, RKL*
Whether managed by your company or outsourced to third-party service providers, staying compliant with growing regulatory demands and multiple security standards requires maintaining and monitoring the proper controls.
We will discuss:
- How to identify the difference between various standards, including but not limited to CMMC, ISO, PCI DSS and SOC
- Tips to manage controls, whether maintained internally or outsourced to third-party service provides, to ensure compliance

10:15 a.m. **Refreshment Break — Exhibits Open**

10:30 a.m. **The 3 W's of Penetration Testing (Pen Test)**
– *Joel Prentice, Security Engineer, Appalachia Technologies, LLC*
A penetration test, known as Pen Test, is a simulated cyber-attack against your computer systems to identify exploitable vulnerabilities, so you can fix them. We will discuss:
- Why do a Pen Test and how do you set it up
- What to expect from a Pen Test; how to use the results to begin fixing any vulnerabilities
- When is the right time to do a Pen Test

11:15 a.m. **Common Data Breaches Faced by Businesses**

– *Sean Stajkowski, Intelligence Analyst II, Pennsylvania State Police, Bureau of Criminal Investigation*

As we enter our third year of the pandemic, cyber crimes against companies are at an all-time high and escalating rapidly. We will discuss:

- What are the most frequent attacks occurring to PA businesses?
- Are there any forensic solutions companies can take to protect themselves?
- Are there any surprises that IT professionals should know about?
- Best practices that help protect companies from the most frequent attacks will be reviewed.

12:00 Noon **Lunch — Exhibits Open**

12:45 p.m. **Keynote: Legal IT Considerations and Challenges Facing Companies**

– *Ronald Plesco, Partner, Intellectual Property and Technology Practice, DLA Piper*

Ronald Plesco, a former prosecutor, is an internationally known information security and privacy lawyer with more than 20 years of experience in cyber investigations, privacy, threat intelligence, information assurance, identity management, cyber threats and cyber-enabled frauds, data analytics and artificial intelligence. With his vast global experience, he will present:

- What are some of the new changes companies are making to IT Departments, and what is forecast that IT professionals should concentrate on moving forward? Examples are companies are moving to decentralizing; how companies are dealing with the severe labor shortage, and more
- An overview of the expanding threat landscape including the rise in social engineering attacks; and the increasing acceptance by companies that the "net zero" attack will come in the next 10 – 15 years, yet companies are not prepared
- A discussion of the most prevalent IT legal challenges facing companies
- Strategies and best practices companies should consider for future protection

1:45 p.m. **Final Questions**

– *Adam Friscia, Membership and Events Executive, PA Chamber*

2:00 p.m. **Adjourn**

Continuing Education Credits

(ISC)^2 CPE Credits

This program has been approved by the International Information Systems Security Certification Consortium, Inc. for **4 (ISC)^2 CPE credits**.

Attorney CLE Credits

This program has been approved by the PA Continuing Legal Education Board for **4 hours of intellectual property law CLE credit** and 0 hours of ethics, professionalism or substance abuse CLE credit.

Accountant CPE Credits

CPE Credits: 4
Program Sponsor PX177225
Prerequisites: None
Level: **Specialized knowledge and applications**
Objective: To provide practical information and best practices on how companies can better manage Information Technology responsibilities and costs, as well as limit liability by improving data security to protect customer and financial information.

About the Speakers

Kate Davenport is the lead Digital Forensics Examiner at Information Network Associates, Inc. (INA), an international investigative and corporate consulting firm located in Harrisburg, Pennsylvania.

Ms. Davenport has a B.A. from McDaniel College and a Professional Certificate in Computer Forensics & Digital Investigation from Champlain College. She is an EnCase Certified Examiner (EnCE) and holds the Cellebrite Certified Operator (CCO) and Cellebrite Certified Physical Analyst (CCPA) certifications from Cellebrite.

Ms. Davenport is the former Digital Forensics Examiner for the Missouri State Public Defender (MSPD), where she established a digital forensics lab in accordance with national standards, writing SOPs for evidence management, acquisitions, and tool testing. Her work at MSPD included performing historic cell site analysis, examining devices, and consulting and reviewing discovery, all essential for case preparation for the assigned attorneys. Also at MSPD, she visited FBI and law enforcement labs to perform defense reviews of hard drives and mobile devices for cases involving child pornography. While at MSPD, she discovered a forensic software anomaly and collaborated with NIST to report it.

Ms. Davenport previously worked as a Forensic Technology Associate at BDO Consulting, where she performed field and lab collections as part of a national forensic team. She employed best-evidence practices during fast-paced investigations involving high-profile clients.

Ms. Davenport joined INA in June 2018, to manage their Digital Forensic Unit. She oversees a variety of digital forensics cases including computer, mobile, and cloud forensics. She also conducts historic cell site analysis. She is available to review forensic reports, perform digital forensic examinations, for general consultation regarding cases, to testify, and to give presentations.

Michael McAllister is a Partner and Leader of RKL's IS Assurance and Advisory Services Practice. With more than 24 years of experience in accounting and computer science, Michael builds the knowledge bridge between the financial aspects of accounting, and the information technology systems and controls that support each process. He serves clients in a variety of industries, ranging from manufacturing to retail, technology and financial institutions, bringing an extensive background in resolving information security and financial audit risks. The core services provided by Michael and his team include: information technology internal audits; IT governance, reevaluation and design; and QA/IV&V (Quality Assurance, Independent Verification and Validation) engagements. In addition, Michael also boasts deep expertise in System and Organization Control (SOC) services, which include control readiness assessments and gap analysis for SOC 1 and SOC 2 reports. Michael provides SOC services for various types of entities, ranging from national service bureaus, financial institutional support entities and data hosting services.

Ronald Plesco is a Partner with the law firm of DLA Piper, where he oversees the Intellectual Property and Technology Practice. A former prosecutor, Ronald is an internationally known information security and privacy lawyer with more than 20 years of experience in cyber investigations, privacy, threat intelligence, information assurance, identity management, cyber threats and cyber-enabled frauds, data analytics and artificial intelligence. Ronald previously served as CEO of the National Cyber Forensics & Training Alliance (NCFTA), where he managed the development of intelligence that led to more than 400 worldwide cybercrime 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.

Ronald also previously served under Governor Tom Ridge as the Director of Public Safety Policy for Pennsylvania. Immediately after 9/11, he was also selected to serve as chair of the Cyber Attacks Committee for the Pennsylvania Homeland Security Council. He also supported Secretary Tom Ridge at the US Department of Homeland Security in the development and deployment of the National Cyber Security Division, US-CERT, TSA Secure Flight and US-VISIT programs. Prior to joining DLA Piper, Ron was a Principal in KPMG's Cyber Services practice and concentrated on the healthcare, manufacturing, financial, insurance, retail, and automotive industries. Ron joined KPMG in 2012 after a distinguished career in the private and public sectors and is a frequent speaker internationally.

Joel Prentice is the Security Engineer for Appalachia Technologies, where his specialty is in penetration testing and malware analysis. Before joining Appalachia Technologies, he served as the Systems Administrator for Eurofins Lancaster Laboratories, and in Advance Technical Support for AT&T Mobile. He holds his Master's degree in Cloud Computing Technology from the University of Maryland.

Sean Stajkowski is an Intelligence Analyst for the Pennsylvania State Police, Pennsylvania Criminal Intelligence Center (PaCIC), as a member of the Critical Infrastructure and Key Resources Unit. His sector concentrations include emergency response planning and monitoring in the areas of transportation and energy across the Commonwealth of Pennsylvania. Sean has participated in emergency preparedness meetings, various cyber threat trainings, and safety presentations for the energy and transportation sectors. He also monitors cyber threats against Pennsylvania infrastructure. He has provided presentations on insider threats, current cyber threat trends, and suspicious activity reporting. Sean holds a Bachelor of Arts degree as well as Master of Science degree in Criminal Justice from Marywood University.

PAChamber™ of Business and Industry

For more information on these events, contact Susan Smith, Educational Services, 717.720.5457 | ssmith@pachamber.org.

For sponsorship information, contact Morgan Roddy, Director of Events & Engagement, 717.720.5428 | mroddy@pachamber.org