ISACA®
Trust in, and value from, information systems
Greater Kansas City Chapter

Information Security Academy

Date: **Tuesday- Thursday -** November 7 – 9, 2017

Time: 8:00 Check In | 8:30 AM – 4:30 PM Presentation

Location: Sprint Nextel World Headquarters – Overland Park, KS
(Additional parking and building information will be provided to registered attendees)

CPE's: 24 Credits

Price: ISACA Members **Early-Bird through October 10th**: $650 – **After October 10th**: $750
Non-Members: $750

Registration: http://www.isaca-kc.org/events **Seating is limited. Register early to secure your spot. <u>Registration closes on October 30th</u>** Prompt payment is required. Registration includes course materials, which will be provided electronically in advance, and a $20 daily food voucher to be used the day of issuance at the on-site cafeteria for breakfast, lunch, and/or snacks.

<u>Presentation Overview</u>: MISTI Learning Level: Intermediate
This three day event will guide you through the basics of establishing and managing an information security program in today's business environment. This class will cover internal and external threats, effective security policies, contingency planning, legislation, regulations, employee privacy issues, awareness programs and more. You will learn about emerging security architectural issues and technologies to assist you, how they can affect computer security in your organization, and what you can do to provide a secure environment as technologies evolve.

Participants will learn the components of a comprehensive strategy, covering such critical areas as planning and managing a security program, getting the business more involved with information security, developing an enterprise security architecture, establishing identity and access control management and network perimeter protection, ensuring physical protection of your business and computing facilities, and complying with the legal and regulatory aspects of information security. The agenda will focus on risk analysis and business impact analysis (BIA) as tested methodologies for measuring the level of security risk and prioritizing information risk reduction in your organization. You are invited to bring your own information risk analysis evaluation criteria and targets, and explore how you can make best use of today's techniques.

In addition, if you audit the security environment, this course will help you identify the essential elements that need to be developed and in place for your organization to maintain effective controls. Throughout the seminar videos, real-life scenarios and case studies will reinforce learning. You will leave this pragmatic course with a blueprint for building an effective information security program or for measuring an existing one. Refer to **Appendix A** for further details.

<u>Speaker Summary</u>:
Mary G. Siero is an executive level Information Technology Consultant and the President of Innovative IT, a Las Vegas based information technology consulting firm. She has over 30 years' experience in engineering and technology from industries such as Healthcare, Government, Gaming and Hospitality, Consumer Products, Manufacturing and Education.

Mary's career includes ten years in healthcare as a Chief Information Officer and five years in the gaming industry as Vice President of IT Operations, both heavily regulated industries.

She is active in the information system security community and has provided testimony on the record for the State of Nevada Information Technology Board regarding The Current and Future Cyber Threat. She routinely presents at national conferences on information technology topics and holds several professional IT security certifications.

She is a Charter Member of the FBI Citizen's Academy Alumni Association in Las Vegas, the Cybersecurity Program Committee Chair for the Las Vegas Chapter of the Society for Information Management (SIM), and is a member in good standing of the International Information Systems Security Certification Consortium (ISC)2, the Information Systems Security Association (ISSA), the Healthcare Information Management Systems Society (HIMSS) , the Information Systems Audit and Control Association (ISACA), Southern Nevada InfraGard Members Alliance ,and Toastmasters .

She is a graduate of the University of Detroit with a Master's Degree in Polymer Chemistry and a graduate of Michigan State University where she obtained her Bachelor's Degree in Chemistry.

The information presented and included in accompanying materials (if any) is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although the speaker and content authors endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Appendix A : What You Will Learn:
DAY ONE

1. Review of Information Security Concepts
  - Goals of information security
  - Fundamental principles of information security
  - Information security management objectives

2. Information Security Department
  - Defining the information security department charter
  - Functions, roles, and responsibilities
  - Security management cycle
  - Staffing your information security department
    - i. Information security certifications overview
      - ISC(2) - CISSP, SSCP, CCSP, HCISPP, etc.
      - ISACA - CISA, CISM, CRISC, CGEIT, CSX, etc.
      - EC Council - CEH, CCISO, CHFI, etc.
      - SANS - GSEC, other GIAC certs
    - ii. Developing job descriptions
    - iii. Hiring the right people

3. Legal and compliance obligations
  - Security vs. Privacy
  - Federal, state, and local laws
    - i. HIPAA, GLBA, FERPA, FISMA, CJIS, etc.
  - Regulatory compliance
    - i. PCI DSS, SEC, SOX, etc.
  - European Union Data Protection Act
  - Intellectual property, copyright laws and software piracy
  - others

4. Information security standards and frameworks
  - NIST, PCI DSS, COBIT for information security, ISO, Critical Security Controls for Effective Cyber Defense, OWASP, CSA, etc.

5. Managing the **Technology**
  - Secure network design
    - i. Enterprise security architecture
    - ii. 3-layer simplified network protocol model
    - iii. Open Systems Interconnection (OSI) model
    - iv. Transmission Control Protocol/Internet Protocol (TCP/IP): IPv4, IPv6
    - v. Wireless networks technologies, protocols, and security
    - vi. Voice over IP (VoIP)
  - Network management tools
  - VPNs and related Internet security protocols: SSL/TLS, IPSec, SSH
  - Security technologies and tools
    - i. Firewalls and proxy servers
    - ii. IDS/IPS
    - iii. Data loss prevention software (DLP)
    - iv. SIEM solutions
    - v. Etc.
  - Cryptography
    - i. Encryption algorithms and hashing functions
    - ii. Digital signatures
    - iii. Key management: asymmetric, symmetric
    - iv. Certificate Authorities (CAs) and Public Key Infrastructure (PKI)
  - Application development tools
    - i. Source code management

The information presented and included in accompanying materials (if any) is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although the speaker and content authors endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

- Cloud security

DAY TWO

6. Managing Security **Processes**
- Information Security Governance
    i. Developing, selling, and implementing a governance program
    ii. Data classification
    iii. Policies, procedures, standards, guidelines
    iv. Decision making processes
- Identity and access management;
    i. provisioning and deprovisioning
    ii. remote access
- Asset, configuration, and change management
- Threat and vulnerability management; log management and monitoring
- Secure software development
    i. software development lifecycle
- Incident and problem management
    i. investigations
- Data protection and management
    i. Database types and models
    ii. Media management, sanitization, and protections
- Disaster Recovery and Business Continuity
    i. Business impact analysis
- Physical and asset security
    i. Data center environmentals
    ii. Physical access controls
- Risk management
    i. Security testing

7. Managing the **People**
- Information security awareness programs
- Human resources security: hiring practices, sanctions, terminations, and transfers
- Position risk assignments

DAY THREE

8. Risk Based Approach
- How hackers attack: the cyber security kill chain
- Assessing threats to information security and areas of vulnerability
- Risk identification, analysis, and management: threats, vulnerabilities, risks, and countermeasures
- Mobile code security risks
- Cloud security risks
- Arriving at an "acceptable level of risk"

9. Third Party Security Management
- Strategies and controls for managing security of third parties
    i. Contracts
    ii. Audits/attestations
    iii. Minimum standards

10. Metrics
- Good vs. bad metrics
- Operational and management reporting

11. Budgeting for information security

12. Communicating and selling information security initiatives
- Communication to the Board
- Management presentations

The information presented and included in accompanying materials (if any) is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although the speaker and content authors endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.