

## **Bios**



**Daniel Morrison**

Dan has over twenty years of industry experience designing and implementing technology and security solutions in all areas of information technology, with specialties in performance improvement, risk management, privacy, infrastructure and application security, advanced card technologies, and biometrics - within financial services, healthcare, insurance, manufacturing, and government organizations.

Dan's focus is on helping companies realize business value by leveraging technology and implementing process improvements that provide measurable results in terms of increased revenues, decreased cost, decreased time-to-market, reduced risk and improved quality.

Prior to PwC Dan worked for American Express as Chief Security Strategist where he created and led American Express Security and Privacy consulting practice. Dan also led the Security Engineering Initiative as a Senior Vice President with Bank of America, and as a Partner with Arthur Andersen, Dan was responsible for providing the global leadership and direction for Information Security Products and Services.

Dan is a Certified Information Security manager (CISM) and Certified Six Sigma Professional who has participated and managed projects throughout the United States, Canada, South Korea, Japan, South Africa and Europe.

Dan has been a speaker at many conferences and has published numerous information technology security related papers. Dan is also a member of the American Bar Association (ABA), the Information Systems Audit and Controls Association (ISACA), the Armed Forces Communications and Electronics Association (AFCEA), and the Computer Security Institute (CSI).

## **Presentation Overview**

**Vendor Security Risk Management:** This session will explore methods, techniques and approaches to allow organizations to quantify and manage vendor security risk. Security risks are related to vendors need to be addressed in a number of Vendor Relationship Management Life Cycle areas. This presentation will examine security risks specific to:

- a) Planning:
  - i) Defining security requirements
- b) Contracting:
  - i) Initial Assessment
  - ii) Minimum Controls
  - iii) Metrics
- c) Vendor Management:
  - i) Problem Management
  - ii) Continuous Monitoring
  - iii) Metrics Dashboard
  - iv) Ongoing Assessments
- d) Vendor Sunsetting
  - i) Transition
  - ii) Information and Asset Recovery
  - iii) Post Contract Controls