JENNIFER L. BAYUK

jennifer@bayuk.com

PROFILE A technology risk management thought leader and cyber security subject matter expert. Experienced in information technology governance, BASEL operational risk management principles, system security architecture, cyber security tools and techniques, cybersecurity forensics, audit of information systems and networks, and business continuity processes. Skilled in cybersecurity risk and performance indicators, technology risk awareness education, risk management training curriculum, and system security research. Masters degrees in Philosophy and Computer Science. Ph.D. in Systems Engineering. Certified in Information Systems Audit, Information Systems Security, Information Security Management, and IT Governance (CISA, CISSP, CISM, CGEIT). NJ Licensed Private Investigator.

EXPERIENCE

Independent Technology Risk Management Consultant, New Jersey, 6/08 to present

Engaged in a wide variety of projects ranging from security policy and metrics for financial institutions to research in systems security engineering for government contractors. Perform cyber security risk and regulatory compliance assessments. Develop systems security architecture. Develop and teach courses in various aspects of cyber security for academic institutions and industry associations. Lecture at conferences. Participate in public and private security-related committees. Assist entrepreneurs on Cybersecurity Architecture, Technology Risk Management, and secure Cloud and Mobile requirements. Provide expert witness and legal consulting services. Exemplar projects:

ISACA NJ Chapter, 3/09-present.
Develop and teach courses on emerging topics in cybersecurity and technology risk and controls.

G. A. Baird Partners & Co, Stamford, CT, 6/17-11/17.
Created Cybersecurity and Technology Risk programs for a *denovo* Bank. Specified systems security architecture for Digital Banking Architecture and Third Party Integration, focusing on Cloud and Mobile Security Technologies.

Stevens Institute of Technology, Hoboken, NJ, 9/09-06/12.
Created a new graduate curriculum in cyber security for the School of Systems and Enterprises, including complete content for four new courses in systems security architecture and engineering. Led three research projects in systems security engineering, including a research roadmap for the Department of Defense Systems Engineering Directorate. Created a systems security engineering laboratory. Taught graduate courses in enterprise security architecture and information security management for the School of Technology Management.

Delta Risk, Chicago, IL, 7/09-1/13.
Provided business requirements, testing, and analysis for Securities Industry and Financial Markets Association (SIFMA) Quantum Dawn Cybersecurity Exercises. Assisted in the development of DECIDE simulation environment for experiencing cyber attack scenarios, and the scenarios used by SIFMA.

Managing Director, Cybersecurity Governance, Risk &Control, JPMorgan Chase, NY, NY, 10/16 to 6/17.
Designed, managed, and measured a Cybersecurity Risk Management framework in support of $600M Firmwide Cybersecurity Program. Managed the evolution of cybersecurity and technology risk policies and standards in coordination with cybersecurity product managers and the broader Technology Control organization. Globally coordinated cybersecurity regulatory, audit, client, and partner engagement in coordination with Technology Control and Cybersecurity Regional leads. Managed governance and control processes applicable to the Cybersecurity organization, including but not limited to self-assessment, resiliency and recovery, issue management, third party oversight, and inter-affiliate agreements.

Managing Director, Operational Risk Management, Citi, New York, NY, 3/13 to 10/16.
Coordinated activities within first and second lines of defense to identify, measure, monitor, and manage key operational risks within Citi's Enterprise Operations and Technology (O&T) division in accordance with firmwide Policies and Procedures (~60 distinct Global and Regional operational entities). Proactively engaged individuals at all levels of management to understand and assess both inherent and residual risk due to business dependency on technology and centralized operations such as Human Resources and Financial Services. Participated in risk-related forums, including the Information Security Committee and Fraud Oversight Committee. Advised multiple levels of executives on a wide variety of topics related to global risk management program strategy and execution. Escalate and track issues. Devised and directed the development of Technology Oversight Procedures and Technology Metrics used firmwide for Management Control Assessment and Operational Risk Analysis.

Senior Managing Director, CISO, Bear Stearns & Co., Inc., Whippany, NJ, 4/98 to 6/08.
Designed and implemented firmwide processes to protect, detect, and recover from harm to information. Established and maintained enterprise-wide security, change control, and business continuity metrics. Chair of the Firmwide Information Protection Committee and member of the Global Outsourcing and Firmwide Emergency Response Committees. Drafted, negotiated, and issued global security policies and processes. Devised tools, techniques, roles, responsibilities, and awareness materials for all security processes including digital identity, application inventory and information systems risk management. Provided technical requirements and test programs for new security products and security features of new applications. Directed the activities of development and infrastructure officers globally with respect to security tools and techniques. Directed information security investigations and remediation activities in coordination with human resources, legal and compliance. Coordinated emergency response teams for information security related events. Reviewed physical security efforts in support of data center protection. Contracted and managed penetration tests. Guided management through information technology (IT) audits. Performed due diligence in support of merger, acquisition, research analyst, and investment banking activity. Testified on due diligence efforts when required by regulators. Prepared materials on security measures for prospective clients. Coordinated industry efforts in support of firm goals for information security improvements. Directly managed department budget (~3M) and security tollgates over all projects in IT budget (~600M). Chief Information Security Officer title achieved in 2002.

Manager, Information Systems Business Controls, AT&T Capital Corporation, Morristown, NJ, 2/97 to 4/98.
Led and executed the company's global internal audit and control assessments with respect to information systems. Conducted security investigations. Provided direction and guidance on systems control issues for the company's strategic leaders, including the Technology Leadership Team and corporate legal counsel. Developed COSO & COBIT compliant systems audit approach for AT&T Capital that includes quantitative communication of systems vulnerabilities. Evaluated and developed tools for operating system, database management system, and network security testing as well as data analysis, incident tracking, and reporting.

Information Systems Risk Manager, Price Waterhouse LLP, Morristown, NJ, 1995 - 1997.
Managed a wide variety of security consulting and audit projects for the Price Waterhouse Information Systems Risk Management Practice, including penetration tests and physical infrastructure reviews. Performed systems infrastructure analysis directed at improving technical security architecture, security management processes, and information system operational risk management. Developed methodology for evaluating the effectiveness of security management processes and trained both consultants and senior managers on its use. Wrote and customized programs for security testing. Evaluated various types of commercial security software.

Information Security Technical Staff, AT&T Bell Laboratories, Holmdel, NJ, 1990 - 1995.
Led diverse, cross-organizational teams focused on security and data integrity, including the AT&T Network Security Requirements Team, the Security Analysis of the Network Environment Team, and the Security Assessment Team. Envisioned, designed, specified, developed, demonstrated, tested, and documented software for expert systems, graphical user interfaces, databases, and network monitors. Spent most of the last year at AT&T with the CFO Organization in Short Hills performing computer security audits and corporate security consulting for various systems comprising and supporting the AT&T Worldwide Intelligent Network.

EDUCATION

PhD Systems Engineering, Stevens Institute of Technology, 2012, Thesis: Measuring Systems Security, GPA 3.9.
MS Computer Science, Stevens Institute of Technology, 1992, GPA 3.9.
MA Philosophy, The Ohio State University, 1986, GPA 3.5.
Thesis compared logic in expert systems to that of compiler design.
BA Computer Science and Philosophy, Rutgers College, Rutgers, the State University of New Jersey, 1985, GPA 3.59, Henry Rutgers Honors Scholar, Thesis in Philosophy of Expert Systems, Rutgers Academic Life Scholarship.
Certified Information Systems Auditor (CISA), 1996.
Certified Information Security Manager (CISM), 2002.
Certified in the Governance of Enterprise IT (CGEIT), 2008
Certified Information Systems Security Professional (CISSP), 2008.

CURRENT AFFILIATIONS

Information Systems Audit and Control Association (ISACA), author/instructor/contributor on a wide variety of topics, conference committee member, author, and exam question contributor. COSO Enterprise Risk Management Advisory Committee, representing Information Systems Audit and Control Association (ISACA)

PAST AFFILIATIONS

Financial Services Sector Coordinating Council (FSSCC.org), member, chair of Research & Development Committee 2006-08.
Metricon Program Committee Member, and Chair for Metricon 4.0, MiniMetricon 5.5 (www.securitymetrics.org).
Information Security Forum (securityforum.org), member, participant in Information Security Architecture Project.
IEEE Computer Society, member, participant in Smart Grid Vision Project.
International Council on Systems Engineering (INCOSE), co-chair, Security Working Group, 2010-2011.
Securities Industry and Financial Markets Association(SIFMA), Information Security Committee Chair, 2003-2008.

BOOKS

Planned 2018	Tentative book title: *Financial Cybersecurity Risk Management,* coauthor, Springer.
April 2012	*Cyber Security Policy Guidebook,* lead of five authors with different areas of Cyber Security Policy Expertise, Wiley.
September 2010	*CyberForensics, Understanding Information Security Investigations,* edited this collection of articles by industry experts and provided an introductory framework, Springer.
January 2010	*Enterprise Security for the Executive: Setting the Tone at the Top*, Praeger.
March 2009	*Enterprise Information Security and Privacy,* Artech House, co-edited this collection, and wrote chapter on "Information Classification."
November 2007	*Stepping Through the InfoSec Program,* Information Systems Audit and Control Association (ISACA), peer-reviewed book.
January 2005	*Stepping Through the IS Audit, A Guide for Information Systems Managers, 2nd Edition*. Book published by the Information Systems Audit and Control Association.
January 2000	*Stepping Through the IS Audit, A Guide for Information Systems Managers*. Book published by the Information Systems Audit and Control Association (ISACA).

COURSES DEVELOPED, LISTED BY INITIAL LAUNCH

Planned June 2018	*Technology's Role in Enterprise Risk Management,* Information Systems Audit and Control Association, NJ Chapter
June 2015	*Loss Capture for Technology-Related Events,* Citigroup Internal Online Training.
January 2015	*Technology Oversight Procedures,* Citigroup Internal Online Training.
August 2014	*Manager's Control Assessment,* Citigroup Internal Online Training.
June 2014	*Information Security Architecture,* Citigroup Internal Online Training.
November 2013	*Information Security Metrics,* Citigroup Internal Online Training.
March 2012	*System Security Management,* University of Virginia's Accelerated Master's Program in Systems Engineering.
June 2012	*Information Security Governance at Board Level*, joint seminar for ISACA & IIA New Jersey Chapters.
April 2012	*Security Documentation*, ISACA Philadelphia & New Jersey Chapters Spring Conference.
Spring 2011	*Systems Security Architecture and Design*, Stevens Institute of Technology
Spring 2011	*Fundamentals of Security Systems Engineering*, Stevens Institute of Technology
Spring 2011	*Secure Systems Laboratory*, Stevens Institute of Technology
June 2010	*Metrics That Actually Improve Security*, Computer Security Institute.
Spring 2009	*Secure Systems Foundations*, Stevens Institute of Technology
March 2009	*Information Security Metrics,* Information Systems Audit and Control Association, NY Chapter
March 2009	*Information Security Governance,* Information Systems Audit and Control Association, NJ Chapter
January 2009	*Information Asset Classification,* Information Systems Audit and Control Association, NY Chapter.
April 1998	*CISA Exam Certification Course*, Domain 4: Information Systems Integrity, Confidentiality, and Availability, ISACA North Jersey Chapter (Also taught in April 1999 and April 2000).

SELECT OTHER PUBLICATIONS & SPEAKING ENGAGEMENTS

March 2013	*Security as a Theoretical Attribute Construct*, Computers and Security, Volume 37.
January 2013	*Measuring System Security*, Systems Engineering, Volume 16, Issue 1, *Best Paper of the Year, #1 Download*.
November 2012	*Overcoming Challenges for Superior System Security Metrics*, ISACA North American ISRM / IT GRC Conference (www.isaca.org).
February 2012	*System-Level Security*, Canadian Financial Institutions Computer Incident Response Team (CFI-CIRT) Annual Conference.
March 2012	*Security via Related Disciplines*, Conference on Systems Engineering Research (CSER).

November 2011	*Measuring Cyber Security in Intelligent Urban Infrastructure Systems*, International IEEE Conference & Expo on Emerging Technologies for a Smarter World (CEWIT).
Fall 2011	*An Architectural Systems Engineering Methodology for Addressing Cyber Security*, Systems Engineering, Volume 14, Issue 3.
July 2011	*Systems-of-Systems Issues in Security Engineering*, INCOSE Insight, Volume 14, No 2.
June 2011	*Cloud Security Metrics*, IEEE Systems of Systems Engineering Conference (SoSE2011).
April 2011	*A Cyberforensics Framework*, The Computer Forensics Show.
March/April 2011	*On the Horizon - System Security Engineering*, IEEE Security & Privacy Magazine, Volume 9 Issue 2.
August, 2010	*Systems Security Engineering, A Research Roadmap, Final Technical Report*, principal investigator for DoD-sponsored publication for the Systems Engineering Research Center (www.sercuarc.org).
November 2010	*Systems Security Engineering Roadmap*, Rethinking Cyber Security: A Systems-Based Approach, Workshop sponsored by the Center for Risk Management of Engineering Systems and the Institute for Information Infrastructure Protection (I3P), University of Virginia.
October 2010	*The Utility of Security Standards*, IEEE International Carnahan Conference on Security Technology (ICCST).
August, 2010	*Systems Security Engineering, A Research Roadmap, Final Technical Report*, primary author for DoD-sponsored publication for the Systems Engineering Research Center (www.sercuarc.org).
June 2010	*Pairing Organizational Strategy with Security Solutions*, CSO Executive Seminar.
June 2010	*Information Security Metrics*, in Readings and Cases in Information Security Management – Legal and Ethical Issues, Course Technology, edited by Mattord and Whitman.
May 2010	*Systems Security Engineering*, Tenth Annual High Confidence Software and Systems Conference, sponsored by the National Security Agency.
December 2009	*Critical Infrastructure Protection Issues in the Financial Industry*, Global Conference on Systems and Enterprises, Stevens Institute of Technology.
September 2009	*Prevention Is Better Than Cure,* Business Trends Quarterly.
June 2009	*How to Write an Information Security Policy*, CSOonline.com.
May 2009	*Information Systems Audit: The Basics*, CSOonline.com.
May 2009	*Third Party Data Handling*, ISACA Control Journal.
March 2009	*Data-Centric Security*, Computer Fraud and Security.
November 2008	*Security Through a Time of Crisis*, Computer Security Institute Annual Conference.
October 2008	*Key Data Points for IT Governance Metrics*, ISACA IT GRC Conference.
July 2008	*Metrics for Risk Management versus Security Attribution*, Metricon Conference.
June 2008	*Third Party Due Diligence*, Securities Industry and Financial Markets Association (SIFMA) Technology Management Conference.
October 2007	*Utilising information security to improve resiliency*, Journal of Business Continuity & Emergency Planning.
October 2007	*Data Classification, Security and Privacy*, Securities Industry and Financial Markets Association, Internal Audit Division, Annual Conference.
Sept/Oct 2007	*IT Attestation Services: What You Need to Know*, Journal of Corporate Accounting and Finance.
June 2007	*CISM Review Manual, Chapter 5: Information Security Program Management,* Information Systems Audit and Control Association.
October 2006	*The Homeland Security Front,* Securities Industry Association, Internal Audit Division, Annual Conference.
November 2005	*Security Review Alternatives*. The Computer Security Journal, Fall 2005, a Computer Security Institute publication.
October 2005	*Best Practices for Securing and Controlling Offshore Vendors,* Securities Industry Association, Internal Audit Division, Annual Conference.
September 2005	*Internal Security Reviews,* Fourth Annual FDIC Technology Seminar.
June 2004	*Sarbanes-Oxley for the IS Professional,* Securities Industry Association, Technology Management Conference.
October 2003	*Metrics for Due Diligence*, Best In Class Security and Operations Roundtable Conference, Carnegie Mellon Software Engineering Institute.
May 2003	*Security Forum 2003, The Secure Enterprise, Wireless LAN Panel,* Technology Managers Forum.
April 2003	*Introducing Security at the Cradle,* SANS (System Admin, Audit, Network, Security Institute) Security and Audit Controls that Work Conference.

Summer/Fall 2002	*Productive Intrusion Detection*, The Computer Security Journal Vol XVIII, No 3-4, a Computer Security Institute publication.
May 2001	*Security Forum 2001, Information Risk Management, Risk Management and Security Metrics Panel*, Technology Managers Forum.
May 2001	*Measuring Security*, Information Security System Rating and Ranking, an Applied Computer Security Associates (ACSA)Workshop.
January 2001	*Security Metrics*, The Computer Security Journal, Vol XVII, No 1, a CSI publication.
August 2000	*Assurance and Monitoring of E-business: Technical Control Points*, Seminar sponsored by Information Systems Audit and Control Association (ISACA) and the Association of Government Accountants (AGA).
June 2000	*Security Metrics: An Audit-based Approach*, Computer Systems Security and Privacy Advisory Board (CSSPAB) Security Metrics Workshop (Sponsored by NIST, the National Institute of Standards and Technology).
October 1999	*Infrastructure Monitoring Challenges*, 22nd Annual National Information Systems Security Conference.
May 1999	*Successful Audits in New Situations*, ISACA Control Journal, (v.III).
November 1998	*How to Survive an IS Audit*, Computer Security Institute Conference, Chicago, IL.
June 1997	*Oracle Database Control Issues*, Vanguard Information Security Expo, Orlando, FL.
January 1997	*Audit & Control of Sybase and Oracle*, ISACA NY Metropolitan Chapter.
January 1996	*Security Controls for a Client-Server Environment*, ISACA North Jersey Chapter.
July 1996	*Security Hot Topics*, Price Waterhouse Information Systems Risk Management Internal Advanced Training, Tampa FL.
October 1996	*Security Through Process Management*, 19th Annual National Information Systems Security Conference, Baltimore, MD.
June 1996	*Security Controls for a Client-Server Environment*, The EDP Audit, Control, and Security Newsletter (EDPACS).

Many of these publications are available for download at http://www.bayuk.com