EVAN L. WHEELER, MS, CISSP, CRISC, GCFA

Phone: 508.425.6933

Email: ewheeler@ossie-group.org

BUSINESS EXPERIENCE

Director, Information Security – Omgeo, A DTCC / Thomson Reuters Company (2008-present):

After joining this relatively young Corporate Information Security Group, the challenge was to build a risk management program from scratch while still keeping operational projects on track. Responsibilities included preparing the organization for a Level 2 SAS70 certification, interfacing with the SEC during regular audits, developing global security standards and guidelines, and working as a senior incident coordinator. This role also entailed developing a layered enterprise information security architecture and risk assessment framework to define a process for consistent security control identification and implementation for both corporate and product services environments.

Senior Security Consultant – Akibia Network & Security Solutions, Inc. (2006-2008):

As a subject matter expert, I provided expert level guidance to customers in evaluating their security posture. This position primarily focused on performing risk management and assessments, digital forensic investigations, network security architecture design, and application penetration testing for enterprise customers. Typical tasks also involved leading projects such as Internet Risk Assessments, Enterprise Vulnerability Assessments, Malicious Threat Assessments, PCI Audits, Firewall Audits, Wireless Audits, Penetration Testing, Topology Analysis, and Policy Development. This included pre- and post-sales support to the sales team in helping to develop scopes of work and proposals to potential customers. In addition, this role involved building and leading a Digital Forensics team at Akibia, and working with business development to develop other new service offerings for the company. Majors projects included:

Enterprise Security Architect, Federal Reserve Bank System – Extended project to develop reference architectures, design patterns, and risk analysis models to define national standards for network flow control.

Digital Forensic Investigator, Mid-Sized Retail Company – Lead an investigation of a suspected internal system compromise. This included gathering and analysis of evidence, and reverse engineering of malware.

Security Operations Consultant, New Hampshire State Agency – Performed a gap analysis of their incident response capability by identifying deficiencies, and developing policies and workflows to manage incidents.

Senior Network Security Engineer – Corporate Technologies, Inc. (2005-2006):

The primary responsibility of this position was to deliver security and networking deployment services, integration, security patch management and other technical consulting services to meet customer needs. Multi-product projects involved the design and implementation of security and networking technologies such as load balancers, SSL VPNs, DNS appliances, and secure authentication systems into existing or new environments at customer sites. Responsibilities also included developing and delivering professional high quality post-implementation production support documentation and conducting knowledge transfer sessions with customers.

Information Security Engineer – Defense Contractor, WareOnEarth Communications, Inc. (2004-2010):

Supplied technical support for firewall systems, performed network troubleshooting, and provided consulting services to various government sites within a Department of Defense research network. Typical assignments have included application of security policy, design of network architecture, testing of network hardware, and implementation of security devices such as NetScreen firewalls and network IDS systems. In addition, this position has provided me with extensive experience with other network security related hardware and software including Cisco and Nortel. In support of these devices, I have developed custom tools and applications to ease management tasks and provide incident reporting to customers.

Systems Security & Network Field Services – MeadWestvaco Corporation (1999-2004):

Supported the Worldwide IT department for preparation of business cases and performed security testing and assessment of new technologies to fit business needs, focusing specifically on global enterprise network technologies and project management methodologies such as PMBOK. Typical assignments included systems security testing, remote access configuration, network/server administration, and custom application development. As the Lead Developer for the Emerging Technology department, I designed and developed secure web-based enterprise applications to support the diverse business units of MeadWestvaco.

Network Support/Administration – Georgia Institute of Technology (1998-1999):

Implemented and maintained a multi-network environment and participated in forensic investigations in support of three multimedia labs in a Macintosh and Windows NT based environment for the LLC Department of Georgia Institute of Technology.

Information Technology Specialist - Summer Intern for MetLife (1996 & 1997):

Performed security audits for client workstations, diagnosed and documented technical issues, supported financial applications, and provided multiplatform help desk support for trading floor networks and clients. This position afforded me extensive experience supporting the demands of a high availability environment, and gave me the basis for the broad and specific toolset required to succeed in the financial market.

EDUCATION

Master of Science in Information Assurance, Northeastern University

Bachelor of Science, Computer Science & Business Economics, Georgia Institute of Technology

IT Process Transformation Course, IT Service Management Framework, ITIL

Project Management Body of Knowledge (PMBOK) Training, Project Management Institute

Classes in Telecommunications & Networking, UNIX Shell Programming, NJ College of Morris

TECHNOLOGY EXPERTISE

Network & Security:

Juniper/NetScreen Firewalls, IDP Systems, and SSL VPNs; F5 BigIP Load Balancers and WAN Accelerators; Cisco Switches & Routers; Foundry and SMC Switches; Nortel Contivity VPN Concentrators; RSA SecurID & Sign On Manager; Infoblox DNSOne; IPv6 Design ...

Assessment Tools:

NMap; Nessus; Retina; ISS Internet Scanner; Core Impact; Rapid7 NeXpose; Ethereal; Watchfire AppScan; Cisco Router Audit Tool (RAT); Netwox; Sam Spade; Network Stumbler; Kismet; EnCase; Helix; Autopsy …

Platforms & Systems:

Windows NT/2000/XP; Unix (Solaris, AIX); Linux; Mac OS; Wireless PDAs; Norton Ghost …

Development & Database:

Java; J2EE; STRUTS; XML; HTML; WebSphere Studio; Apache Tomcat & Eclipse; Lotus Notes; Visual Basic; MS Access; MySQL; Perl; Tivoli Suite; Cognos Impromptu; MS Project; MS Visio; Macromedia Flash MX …

TEACHING EXPERIENCE

Instructor & Author – SANS Institute (2008 - present):

Course author and instructor for the *MGT 442 Information Security Risk Management* course. Instructor in the SANS Local Mentor Program in the *SEC 508 Systems Forensics, Investigation, and Response* course. Technical reviewer for the new *SEC 427 Browser Forensics* course. Contributed courseware content on risk management, attack methods, data retention concerns, and USB device security to *MGT 512 Security Leadership Essentials for Managers*, in an effort to revise the course to meet CompTIA objectives.

Part-Time Faculty – Northeastern University (2009 - present):

Teaching online courses in *Foundations of Information Security Management* and *CISSP Preparation* for the College of Professional Studies (CPS) Graduate program using the latest in multimedia media technology to enhance learning in a virtual classroom

Instructor – Clark University (2008 - 2010):

Instructor and curriculum author for the Masters of Information Technology program teaching the graduate course *Information Risk Management* to future CIOs and IT professionals

PUBLICATIONS & PRESENTATIONS

“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.” Book, Syngress, May 2011

“Information Security Leadership Development: Building and Managing a Successful Information Security Program.” Workshop, Presenter & Moderator, RSA Conference, February 2011

“Risky Business.” Presentation, Presenter, SANS Boston Conference, August 2010

“Risk Management: The Next Evolution in Security.” Panel Presentation, Moderator, RSA Conference, March 2010

“From Security Insider to Security Consultant.” Peer to Peer Session, Facilitator, RSA Conference, March 2010

“A Crash Course in Security Consulting: The Art of Scoping.” Presentation, Presenter, SANS COINS Workshop, October 2009

“Risk Management Summit: Why Risk Management?” Presentation, Speaker & Panelist, CSI Conference, October 2009

“Changing the Way We Manage Vulnerabilities & Patching.” Webcast, Presenter, SANS Institute, October 2009

“Introduction to Digital Investigations.” Presentation, Presenter, HCC Information Security Awareness Conference, October 2009

“Improving Vulnerability & Patch Management.” Featured Blog Entry, Author, Akibia’s Practical Guide to Enterprise Technology, October 2009

“Computer Forensics, Investigation and Response.” Presentation, Presenter, Maine Telecommunications User Group Conference, May 2009

“Architectural Risk Analysis – A Practical Approach.” Panel Presentation, Moderator, RSA Conference, April 2009

“How to Prepare for the Five Most Common Security Investigations.” Panel Presentation, Moderator, RSA Conference, April 2009

“Shifting the IT Focus: From Security to Risk Management.” Presentation, Speaker, Clark University Seminar Series, January 2009

“Assessing Your Organization’s Forensic Readiness.” Presentation, Speaker, CSI Conference, November 2008

“Plan in Advance for a Forensic Investigation.” Panel Session, Moderator, RSA Conference, April 2008

“Watching Out For Big Brother.” Article, Referenced & Quoted, Human Resource Executive, October 2007

“CSI for the CSO.” Article, Referenced & Quoted, Information Security Magazine, September 2007

“An Introduction to Digital Forensics.” Article, Author, Bandwidth Network & Security Publication, 2007

“Digital Forensics in the Enterprise.” Webinar, Co-Presenter, 2007

“Preparing for Digital Forensic Investigations.” Presentation, Presenter, Boston Network Users Group, 2007

“CSI for the Enterprise.” Presentation, Presenter, Maine Telecommunications User Group Conference, 2007

Information Assurance Summer Seminar Series. Workshop, Lecturer, Northeastern University, 2007

“Payment Card Industry Compliance: Best practices from successful audits.” Webinar, Co-Author, 2006

MEMBERSHIP IN PROFESSIONAL ORGANIZATIONS

Member of High Technology Crime Investigation Association, HTCIA, 2009

Member of SANS Advisory Board, SANS Institute, 2007

Member of FBI’s InfraGard Association, InfraGard, 2006

Member of Information Systems Security Association, ISSA, 2004

AWARDS & RECOGNITION

President’s Club Winner, Akibia Network & Security Solutions, 2008

Ambassador Club Winner, Akibia Network & Security Solutions, 2007

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP), ISC^2
Certified in Risk and Information Systems Control (CRISC), ISACA
Systems Security Certified Practitioner (SSCP), ISC^2
GIAC Certified Forensics Analyst (GCFA), SANS GIAC
GIAC Security Leadership Certification (GSLC), SANS GIAC
GIAC Security Essentials Certification (GSEC), SANS GIAC
Information Assurance Security Officer (IASO) Certification, U.S. Army School of IT Information Assurance
National Incident Management System (NIMS) Certified, FEMA Emergency Management Institute
Juniper Networks Certified Internet Associate (JNCIA-FWV, JNCIA -IDP, JNCIA -SSL), Juniper Networks
Juniper Networks Sales Specialist in Advanced Security (JNSS-S), Juniper Networks
RSA Certified Systems Engineer – SecurID, Sign-On Manager (RSA-CSE), RSA Security
F5 Certified System Engineer - Local Traffic Management (F5SE), F5 Networks
Certified Infoblox Engineer (CIE), Infoblox
Certified Infoblox Sales Associate (CISA), Infoblox

SECURITY CLEARANCE: Active government clearance level available upon request; issued in May 2005 and renewed in August 2010