

BRUCE A. WESTBROOK

555 Main St., Some City, Some State
555-555-5555 • bwestbrook@gmail.com

INFORMATION TECHNOLOGY SECURITY MANAGER

Certified IT security manager with over 18 years experience in systems operations, security management and IT management. Results driven professional with notable success directing a broad range of corporate IT security initiatives in support of business objectives. Excels at providing strategic direction, IT operations and security management, comprehensive secure network design, risk analysis and regulatory compliance. Able to solve business needs and meet strategic initiatives with enabling technology. 10 years experience in the financial arena securing and monitoring networks and systems that perform \$800 million in transactions per day.

Areas of Expertise:

- Network Design and System Hardening
- Security Information Management (SIM)
- Incident Response
- Regulatory Compliance
- Enterprise Risk Management (ERM)
- Vulnerability Assessment
- Business Continuity (BCS) / Disaster Recovery (DR)
- Intrusion Detection and Prevention (IDS / IPS)
- Physical Security Systems Management
- Unified Threat Monitoring
- Strategic Planning
- Team Leadership
- Project Management
- Senior Management & Board Reporting
- Cost Benefit Analysis
- IT Policy and Procedure Development and Implementation

TECHNICAL PROFICIENCIES

Platforms: Windows (all versions), Linux, Lotus Domino/Notes, Cisco IOS
Databases: MySQL 4.x/5.x, MS SQL 6.5/7.0/2000, Oracle 8x/9i/10g
Languages: Visual Basic, VBScript, DOS batch, Linux bash scripting, HTML, JavaScript, Kixstart, PHP
Security Tools: Ethereal, NMAP, Nessus, GFI LANGuard, MBSA, Trigeo, Tripwire, Snort, ACID, Aanval, Trend Micro, Websense, DansGuardian, BlueCoat, RSA SecurID, RADIUS, SQUID, MailMarshal, Cisco VPN, Fortify, SNMP, Syslog
Firewalls: Cisco PIX, Raptor (Eagle, Raptor and Symantec versions), Sonicwall Pro, Linux iptables (command line & front-ends, incl. IPCop & Endian Firewall), Sentryware HIVE
Systems Managed: Cisco Routers, Foundry Switches, NetApp NAS, EMC Clariion SAN, Intertel PBX, Mercom Call Recording System, WinPAK

PROFESSIONAL CERTIFICATIONS

CISM Certified Information Security Manager (ID# 381577)
CISSP Certified Information Systems Security Professional (ID# 94319)
MCSE Microsoft Certified Systems Engineer (MCP# 394773)
CCNA Certified Cisco Network Associate (ID# CSC010170902)

“Bruce Westbrook is one the best IT Security Managers I have seen in my 15 years providing services to organizations. He pays strict attention to detail, has a deep knowledge and understanding of technical issues and the real world risk of IT security. Bruce has always been open, friendly, communicative and professional. He has strong personal and professional ethics and a knack for ensuring that his IT environment is the highest quality possible. I would recommend him for any IT or security position. If you need a "go to" guy, Bruce is the one for the job.”

Brent Huston, CEO, Microsolved Inc.

PROFESSIONAL EXPERIENCE

NexGen Systems, Inc. – Westerville, OH

1999 - Present

President / CTO, 1999 – Present

Primary leadership for this locally successful technology consulting firm providing IT networking and security services to small and mid-sized businesses. Drive performance in the areas of marketing, operations and hands-on consulting with a strong, principal focus on service quality and customer retention. Manage multiple 1099 consultants and all financial records and reporting.

Major Contributions:

- Orchestrated company start-up and growth to a consistent and manageable state, while simultaneously putting forth 100% effort into a full-time career path.
- Achieved and maintained superior levels of customer satisfaction by ensuring the continuous delivery of top quality services.
- Redesigned customer network and remote access capabilities, moving them into compliance with HIPAA regulations and additionally increasing their productivity capabilities by 300%.
- Orchestrated infrastructure build-out, structured cabling installation and telecom services provisioning to move architectural firm data center to a new location, successfully completing the build-out, move and restoration of all computing services on time and under budget.

SANITIZED Financial Organization

1997 - Present

AVP IT Systems Security, 2006 – Present

*** Rehired to sensitive security position within financial organization with full tenure and relocation.* Provide vulnerability assessment of all systems, applications and networks. Ensure the safety and security of data through ongoing risk analysis. Develop and deliver a new security strategy focused on enclave computing. Oversee systems operations and application development in ensuring security concepts are properly implemented in a repeatable and consistent basis. Actively participate in communication with senior management as a member of the Information Security Oversight Committee. Ensure IT compliance with NCUA Section 748 and Graham-Leach-Bliley (GLBA) regulations, as well as FFIEC guidelines.

Major Contributions:

- Researched and established standardized business process for identity and access management (IAM). Ongoing effort to reduce IT administration, improve security and user productivity, and more efficiently produce compliance reports through technical implementation of IAM.
- Decreased costs substantially through evaluation and ultimately replacement of outsourced network monitoring, resulting in cost savings of \$96,000 annually.
- Created procedures for and assisted the Bolivian central credit union with securing new SSL certificates for their Tomcat based secure financial transaction site, thereby ensuring uninterrupted service to their members.
- Architected and deployed a 500 point honeypot network with real-time alerting, successfully replacing high maintenance and high false-positive IDS/IPS systems. Achieved very high accuracy alerts with less than 1% false positives, providing true actionable event notification.
- Developed process to securely distribute monthly board reports via electronic means, thereby reducing printing costs and increasing productivity by allowing board members to view the material prior to meetings.
- Implemented a redesigned DNS architecture that more securely segregated multiple DMZs from the internal network, decreasing the possibility of externally mapping the internal network. Additionally this implementation added another security layer against malware by taking advantage of DNS blacklisting, allowing malware to be more quickly identified and removed before further harm or propagation could occur.
- Instituted a formal separation of duties between security controls and risk management, thereby increasing efficient security practices and regulatory compliance.
- Increased customer satisfaction of web services through hands-on migration of higher bandwidth firewalls, resulting in faster connections and dramatically fewer complaints.

SANITIZED Financial Organization**2005 - 2006****Director of Information Technology Operations, 2005 – 2006**

Recruited with full relocation to assist the VP of IT with solidifying the foundation of the IT department and securing the infrastructure.

Major Contributions:

- Secured the core processing system's (OSI) externally facing web interface utilizing various layers, including a leading edge application security firewall (HIVE), thereby achieving a mitigated and acceptable risk level in time for its public release to customers.
- Developed and deployed a web-based change management system using freely available tools (Linux, Apache, MySQL and PHP) to keep cost down, dramatically increasing effective communication within IT which in turn decreased troubleshooting and problem resolution issues.
- Created and documented the 2006 IT initiatives based on the organization's business direction, which plan continues to be implemented to this day even after leaving the organization.
- Redesigned a portion of the internal network that included the deployment of internal, vendor facing IPS sensors which enhanced both the performance and the security of the network.

SANITIZED Financial Organization – Columbus, OH**1997 - 2005****AVP Systems Security, 2003 – 2005**

Provided vulnerability assessment of all systems, applications and networks. Ensured the safety and security of data through ongoing risk analysis. Oversaw systems operations and application development in ensuring security concepts are properly implemented in a repeatable and consistent basis.

Major Contributions:

- Reduced spam email issues through reconfiguration of systems, resulting in 25% increase in spam filtering.
- Researched, architected and deployed a security information and event management system (SIM) to identify, notify and respond to network attacks. Increased regulatory compliance and realized 500% gain in efficiency through log correlation and analysis.
- Conducted required security awareness classes for all employees, including executives, on a semi-annual basis, as well as distributed monthly security bulletins and quizzes that were cognizant of the audience's technical expertise. This activity brought security awareness to the forefront and exceeded regulatory compliance needs.

Manager of Systems Operations, 2001 – 2003

Managed the security and availability all technology operations, including capacity planning, staffing, budgeting, and operating efforts of the IT, telecommunications and security functions for this \$4 billion financial institution.

Major Contributions:

- Deployed the first and only shared branching financial system for the central cooperative in Cochabamba, Bolivia, connecting credit unions across the country and bringing financial access to thousands of Bolivians.
- Optimized network performance by replacing stackable switches with new redundant core switch technology, increasing throughput and minimizing downtime.
- Instrumental in implementing dramatic IT reorganization that lifted morale, improved operational efficiencies, and united the day-to-day operations and technical staff.
- Managed hands-on the end to end process of implementing a completely autonomous disaster recovery site for all financial operations, culminating in successfully running a live days work at the site each and every year.

Senior Systems Administrator, 1998 – 2001

Promoted to oversee systems administration and Tier III support. Contributed to the safety and availability of the network through the development of consistent and repeatable processes. Retained through Y2K as one of only four individuals company-wide to receive a significant 3-year bonus plan to ensure successful ongoing operations.

Systems Administrator, 1997 – 1998

Provided on-site and remote support for internal customers for LAN/WAN applications and systems.

SANITIZED Insurance Company – Grand Rapids, MI**1990 - 1997****LAN Administrator, 1996 – 1997**

Led technical support team in fulfilling responsibilities for system support of PCs, Novell servers, and Nortel PBX. Coordinated PC training to company personnel.

Network Computing Operations Support, 1990 – 1996

Ensured the smooth and continuous operation of insurance claims processing through the support of PC systems and applications and training of personnel.

PROFESSIONAL DEVELOPMENT AND EDUCATION

Certified Information Security Manager (CISM)	2006
Certified Information Systems Security Professional (CISSP)	2006
SANS – Secure Internet Presence (LAMP)	2004
SANS – Incident Handling	2003
SANS – Secure Windows 2000 Migration	2000
Certified Cisco Network Associate (CCNA)	2000
Microsoft Certified Systems Engineer (MCSE)	1999
CTIA A+ Technician (A+)	1997
Microsoft Certified Professional (MCP)	1996
Certified NetWare Administrator (CNA)	1996
Sanitized Business College – Business Administration	1988 – 1989
Sanitized Junior College – Business Administration	1987 – 1988
Sanitized Skill Center – Data Processing	1985 – 1986

PROFESSIONAL ASSOCIATIONS

CUISPA	Credit Union Information Security Professional Association
OWASP	The Open Web Application Security Project
ISACA	Information Systems Audit and Control Association
ISSA	Information Systems Security Association
ISC2	International Information Systems Security Certification Consortium

OTHER NOTES

Books:	Wrote book for Advisor Media, “Designing, Installing and Securing Windows NT for E-Commerce”
Magazines:	Published author with articles in “Security Advisor Magazine”
Speaking Engagements:	2007 – Presenter and moderator of a technology round table for the Ohio Credit Union League with an audience of managers and C-level executives. 2005 – Presenter on Intrusion Detection and Prevention Systems (IDS/IPS) to the Region II IS&T Focus Training for the National Credit Union Association (NCUA) auditors.