

Josh More - Operations Roles in Small Business

Certifications: CISSP, GIAC-GSLC Gold, GIAC-GCIH, RHCE, NCLP, ACE

web: <http://www.starmind.org>

Profile

- Fifteen years technical experience consisting of twelve years in security and ten years in operations.
- Expertise in assessing technology, business requirements and security threats.
- Experience presenting to people at all levels of technical skill and business responsibility.
- Detailed knowledge and experience with system analysis, architecture and operations.
- Dedication to continual self-driven improvement of professional skills.

Experience

November 2004 – present

Alliance Technologies

Operations Management: Focus on Projects and Internal Improvement

- Improved operations through a mix of technologies and process changes.
 - Collaborative documentation system improved employee communication and process documentation.
 - Version control system increased speed and reliability of software development.
 - David Allen's *Getting Things Done* methodology improved efficiency.
 - Network monitoring systems served to move the company in a more proactive direction.
 - Asset management system reduced deployment time and increased licensing compliance.
 - Overhauled email system significantly reduced both delivery and troubleshooting times.
- Overhauled and organized internal office spaces:
 - Hardware Inventory – determined standards for what to keep, organize remaining stock.
 - Data Center – organized layout of Data Center to maximize emergency repair efficiency.
 - Software Inventory – identified and organized software for media control and license maintenance.
- Managed numerous projects for security, compliance, process improvement and reducing costs.
- Led company-wide documentation effort focusing on client and data center infrastructure.
- Overhauled business models and revamped products:
 - Web hosting – focus on services-provided rather than bundling and guesswork
 - Email hosting – outsourced to business partner running Communigate Pro, migrated existing
 - Anti-Spam – transitioned from Postini to Google to TestudoData management, migrated existing
 - Anti-Malware – added service levels, implemented new solution, migrated existing
 - SSL Certificates – simplified offering, saving several thousand dollars annually
- Designed imaging and configuration management solution for the banking industry.
- Managed on-call schedule for all network technicians.
- Overhauled configuration of RADIUS to streamline operations and simplify billing.
- Managed shared data for entire company: data analysis, expiration, archiving and centralization.
- Maintained complex set of Solaris servers and zones for stability and security.

System Architect and Administrator: Focus on Security and Open Source Technologies

- Designed and implemented new server standards for core business services.
- Documented all server configurations, histories, and contracts as part of standardizing operations.
- Analyzed and implemented security patches on 40+ systems monthly.
- Developed Linux-based small business server and services, focus on security and email.
- Designed and led ground-up re-implementation of multi-platform email system:
 - Saved \$80,000 yearly through reduced personnel requirements for troubleshooting and maintenance.
 - Reduced call volume by 90% and spam volume by 95%.
 - Removed numerous mail loops resulting in faster and more reliable email delivery.
- Led the migration, deprecation and centralization of legacy systems.
 - Migrated legacy and unsupported Linux to modern Enterprise-quality Linux.
 - Migrated numerous IIS-sites to a newly built, standardized and secured IIS system.
 - Migrated various databases to secured and recent versions of MySQL and Oracle.
 - Developed standards for PHP, Ruby, Drupal, Joomla, Moodle and Wordpress hosting.
 - Built Ruby on Rails self-managed hosting platform.
 - Overhauled client-focused web statistics system for accuracy, speed and support of new technologies.
- Performed complete reimplementation of genetics processing system, focus on security and stability.

- Assisted with re-implementation of DNS and DHCP system, improving resilience and stability.
- Migrated SCO OpenServer installations to both VMWare and new hardware for archival purposes.
- Created emergency disaster recovery servers for failing but critical clients' legacy servers.
- Configured custom monitoring solution for troubleshooting trend analysis and alerting.
- Rebuilt PGP-based encryption system for FTP transfers of HIPAA-controlled information.
- Set up traffic shaping and multi-routing on Linux-based network appliance.

January 2008 – present

SANS and GIAC

Question Author and Reviewer: GIAC certification exams based on SANS course material

- Wrote and reviewed for the GWEB certification, focusing on web-based security issues.

SANS Instructor (Mentor Level): Management 414 – CISSP Mentor Session

- Taught students the ten domains of Information Security to prepare them for the CISSP exam.
- Emphasized practical security concerns within their respective professional environments.
- Added additional teaching of test taking, studying and memorization techniques.

December 2005 – Present

Pearson Educational, O'Reilly Press, Syngress

Technical Reviewer: Focus on Security and Applicability to the Market

- Reviewed numerous book proposals and recommended for or against publication

Technical Editor and Proofer: Focus on Security and Technical Accuracy

- Proofed *Security+ Review Guide*
- Edited *Novell Cluster Services for Linux and NetWare*
- Edited *FreeBSD 6 Unleashed*
- Edited *X Power Tools*
- Edited *Linux in a Nutshell*

May 1999 – November 2004

Clement Claibourne LC / Mail Services LC

Web Developer / Product Manager

- Migrated workstations to open standards, then to Linux systems, reducing licensing liability.
- Designed, implemented and administered Linux based products and solutions, providing:
 - Web interfaces for the on-line viewing, editing, and printing of statements and letters.
 - Ability to pay on-line via existing e-commerce vendors.
 - Optional inclusion of content-aware banner advertisements.
 - Extensive customizations to allow clients and clients' customers to re-brand systems.
 - Simple creation of buttons and banners for system branding.
 - Web-based management console.
- Dramatically improved security via strong authentication and seamless logins.
- Designed websites for Clement Claibourne, Mail Services and several clients.

Systems Architect / Product Manager

- Transitioned from SCO Unix to joint Linux and Windows systems for considerable cost savings.
- Created customized Linux distributions based on Red Hat Linux technology.
- Designed, implemented and administered Linux based products and solutions, providing:
 - Automated file transfer and email parsing, conversion, and processing.
 - Development and support issue tracking and documentation.
 - Automatic data compression, regaining 90% of system resources.
- Researched, installed, and configured tools to aid business, resulting in large operations savings.
- Increased reliability by upgrading a home-brew system to a standardized Linux distribution.
- Designed and oversaw development of Windows-based print archival system.
- Merged diverse networks together following acquisition by Mail Services LC.
- Managed 20 Linux-based Internet-connected servers and 40+ SCO Unix-based LAN-connected servers.

Community Involvement

Security and Open Source Community Leadership:

- Head of Cyber division of Iowa Infragard: an FBI-vetted business/government collaboration.
 - Ran annual conference focused on security communication and education.
- Founded local Virtualization Users' Group and Des Moines Security Group.
- Hosted and ran meetings as President of the local Linux Users' Group.
- Attend local meetings as a security and technical community representative:
 - Agile Users Group, Iowa Bloggers, ISSA, Cyber Defense Competition at Iowa State University
- Consulted to the State of Iowa Department of Homeland Security Information Technology Group.
- Active on numerous international security-focused mailing lists and IRC channels.

Security and Open Source Community Presentations:

- 2011: Virtual Desktop Security – technologies and issues involved with the security of virtual desktops
- 2011: Senior Scams – issues impacting senior citizens and those that care for them
- 2011: Malware and Identify Theft – short-form presentation on big issues effecting businesses
- 2011: Sales – internal presentation educating sales staff on security strategy and prospecting
- 2010-2011: General – common security issues impacting businesses
- 2010-2011: Finance – financial malware impacting banks and credit unions
- 2010-2011: PCI – compliance issues for small businesses accepting credit cards
- 2010-2011: HIPAA – compliance issues for medical clinics, insurance agents and hospitals
- 2010-2011: Malware – financial malware impacting general business and non-profit groups
- 2010: Communication – network-level issues impacting telephone companies and data centers
- 2009: Disaster Recovery – technical issue overview for the Iowa Contingency Planners
- 2009: GroupWise 8 – features of the new email and calendaring system for an internal audience
- 2009: Web Application Security – general security issues for the Des Moines Web Geeks
- 2009: Virtualization Security – security issues surrounding virtualization for ISSA
- 2009: Linux Security – security issues specific to Linux for Infragard and CIALUG
- 2006-2009: MediaWiki – features and use cases for wikis as collaboration systems
- 2008: Security Policies – overview of security policy issues for ISACA
- 2008: OSX Security – overview of security on Apple computers for Des Moines Mac Users Group
- 2008: SQLi and XSS – overview of web-based attacks for the Iowa Ruby Users Group
- 2008: Information Warfare – review of public data attacks and defense for Iowa Infragard
- 2005-2008: Certification – recommendations for certification paths and testing tips
- 2007-2008: Web 2.0 – business uses of emerging web technologies
- 2007: Barcamp – ran sessions on Linux, monitoring, job searches and self-promotion
- 2006: Guest Lecture – lecture on Linux in business for the DMACC Linux Administration Class
- 2006: Technology for Entrepreneurs – using technology to grow startup businesses
- 2005: Linux in schools – how open source technology can improve education

Open Source Community Service:

- Limited free technology and security consulting for community entrepreneurs.
- Designed and maintained a server which provided web, database and email functions for nonprofits.
- Created, designed and managed various community driven projects and websites:
 - Convention Planning - www.demicon.org (website 2000-2003, codebase 2000-2008)
 - Training for Unix Administrators - trouble-maker.sf.net (2004-2010)
- Designed and implemented a kiosk system with speech synthesis for the visually-impaired.

Nov. 1996 – May 1999

Grinnell College

Technical Support: User Consultant / Help Desk Technician

- Analyzed applications for network inclusion, with a focus on stability and security.
- Audited existing applications for adherence to security requirements.
- Secured Windows and Macintosh systems against unauthorized users and malicious applications.

May 1998 – Aug. 1998

University of Notre Dame

Academic Research: Intern in High Energy Physics

- Programmed system to aid high-energy particle analysis.
- Trained other interns in the use of the Unix operating systems.

Education and Certifications

- CISSP – Certified Information Systems Security Professional
- GIAC-GCIH – GIAC Certified Incident Handler
- GIAC-GSLC Gold – GIAC Security Leadership Certification, Gold Level, Paper available online
- RHCE – Red Hat Certified Engineer (expired)
- NCLP10 – Novell Certified Linux Professional 10
- ACE – Astaro Certified Expert

- February 2011 – Attended *Sophos* online training sessions to attain internal certification level
- January 2009 – Attended *SANS* 504 Hacker Techniques, Exploits and Incident Handling Class
- September 2008 – Attended *Astaro* Engineer Training, achieved Astaro Certified Engineer certification
- May – 2008 – Attended *Microsoft* Licensing training
- January 2008 – Taught *SANS* 414 CISSP Prep Class
- December 2007 – Attended *Compellent* SAN Administration Class
- February 2007 – Attended *SANS* 512 Management class
- December 2005 – Attended *N-Able* Advanced Administration Class

- Bachelors degree in Physics, conferred by Grinnell College
- High Energy Physics Internship, University of Notre Dame