Josh More: Data Security

Certifications: CISSP, GIAC-GSLC Gold, GIAC-GCIH

Profile

I am a security advisor, author and presenter with over 15 years experience in information technology. I focus on Lean and Agile approaches to security challenges, including CISO services, technical assessments and remediation assistance. Through the use of continual improvement techniques, I help businesses increase their security posture over time while minimizing impact to production.

Experience – Full Time

September 2011 – Present *Director of Security Services* *RJS Smart Security*

Security Strategy:

- Created Lean Security strategy for consultancy, from marketing to service delivery, including profitability studies.
- Created flow-based project management methodology for internal use and guiding client projects.
- Devised rapid assessment processes to reduce costs and speed delivery for traditional assessment types.
- Revised traditional security assessments to focus directly on business needs: Data, Disaster Recovery, Compliance.
- Defined Security consulting team's core technology suite, balancing discovery needs against cost to clients.
- Performed CISO services to companies in Development, Financial, Health and Entrepreneurial industries.
- Designed new data assessment process for multi-national hospitality chain.
- Created data security management strategy for development firm's primary product offering.

Security Tactics:

- Assessed vendor technologies to vet solutions for internal and external use: Global Velocity, Bit9, Sourcefire, Barrier1.
- Analyzed legacy ASP.NET/SQL Server application for HIPAA/HITECH compliance with focus on data storage issues.
- Assessed outsourced billing services business to determine changes needed to meet HIPAA/HITECH requirements.
- Designed and managed strategic plan to develop new business units for expanding services to consumer market.
- Performed vulnerability and data assessment for national retirement community management servicer.

November 2004 – September 2011 *Senior Security Consultant* *Alliance Technologies*

Security Strategy:

- Researched public data to detect data leaks and prepare for penetration tests.
- Wrote custom reporting system to save $25,000 yearly in licensing costs.
- Guided intrusion recovery efforts for clients for malware incidents with thefts in excess of $500,000
- Assessed vendors: Encryption, IDS/IPS, Anti-malware, Perimeter Protection, Email Control, Web Filtering, WAF.
- Consulted for compliance with PCI-DSS, HIPAA/HITECH, FDIC, SOX and the FTC Red Flag Rules.
- Provided outsourced Chief Information Security Officer (CISO) duties for medium businesses and enterprises.
- Created emergency disaster recovery servers for failing but critical clients' legacy servers.

Security Tactics:

- Conducted network and web-focused vulnerability scans for companies of all sizes and industry verticals.
- Ran incident management program, focused on isolation, determination and correction of security incidents.
- Performed forensic analysis on corrupted and deliberated deleted data for lawsuits up to $20,000,000.
- Consolidated legacy email, web, database and network support systems for increased security and 90% cost reduction.
- Performed highly complex data and contract analysis of multi-party code escrow dispute.
- Designed system to securely transfer large files between businesses in a user-friendly manner.
- Designed and developed highly hardened Linux systems for Web, FTP and Java hosting, saving $80,000 yearly.
- Managed shared data for entire company: data analysis, expiration, archiving and centralization.
- Maintained complex set of Solaris servers and zones for stability and security.

May 1999 – November 2004 *Product Manager / Security Analyst* *Mail Services Inc / Clement Claibourne*

Security Strategy:

- Implement system standards for Linux, Windows and SCO Unix-based systems.
- Ensured products' technical compliance with the Graham-Leach-Bliley Privacy Act and HIPAA.
- Devised password, role, and data management policies for improved security and privacy.
- Designed and oversaw development of multi-platform and multi-algorithm encryption system.

- Drafted policies for the secure handling of sensitive customer data.

Security Tactics:

- Implemented automatic synchronization to backup systems for redundancy and disaster recovery.
- Automated security maintenance on nation-wide cluster of Linux systems.
- Developed automated file processing system via HTTP, FTP and SMTP parsing, conversion, and processing.
- Automated lossless data compression, resulting in a 90% gain in system resources.
- Managed 20 Linux-based Internet-connected servers and 40+ SCO Unix-based LAN-connected servers.

November 1996 – May 1999 *User Consultant / Help Desk Technician* *Grinnell College*

Security Tactics:

- 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.

Experience – Contract and Volunteer

January 2012 – Present *Author*

- Vendor Assessment Handbook, author, book to be released in 2013
- Job Reconnaissance: Using technology to win the job hunt game, author, book to be released in 2013
- “Using Metaphors for Critical Communication”, author, paper to be released in 2013
- Breaking In To Information Security, co-author, book to be released in 2013
- Lean Security 101, author, comic book released 2012
- UTM Security with Fortinet: Mastering FortiOS, co-author, book released 2012
- “Measuring Psychological Variables of Control in Information Security”, author, paper released in 2011

January 2008 – Present *Exam Author* *SANS / GIAC*

- GIAC Certifications: GWEB, GWAPT, GSLC, GCFA

December 2005 – Present *Author Support* *Pearson Education / Novell Press / O'Reilly Press / Syngress / Elsivier*

- Supported numerous book processes as editor and reviewer: *Liars and Outliers*, *UTM Security with Fortinet*, *Security+ Review Guide*, *Novell Cluster Services for Linux and NetWare*, *FreeBSD 6 Unleashed*, *X Power Tools*, *Linux in a Nutshell.*

January 2006 – Present *Community Leadership and Assistance*

- Head of Cyber division of Iowa Infragard: an FBI-vetted business/government collaboration.
- Ran annual Infragard conference focused on security communication and education.
- Hosted and ran meetings as President of local Linux Users' Group.
- Member of Iowa community groups: Agile Users Group, Iowa Bloggers, ISSA, Cyber Defense Competition at ISU
- Member of Minnesota community groups: OWASP, ISSA, DC612, ISC(2), Practical Agility

Teaching

2005-Present *Presentations*

- Lean Security 201 – Lean/Agile Security practice, at numerous venues throughout 2012 and 2013
- Lean Security 101 – Lean/Agile Security theory and techniques, at numerous venues throughout 2012 and 2013
- Pen Testing Security Vendors – for DerbyCon 2012
- Natural Compliance: PCI and HIPAA – at numerous venues throughout 2012 and 2013
- Credit Card Security – PCI compliance issues for small businesses accepting credit cards
- Health Data Security – HIPAA compliance issues for medical clinics, insurance agents and hospitals
- Information Warfare – review of public data attacks and defense for Iowa Infragard

2008 *SANS MGMT 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.

Skills

Consulting

- Analyze business processes, systems and networks to determine long term security strategies at minimal cost.
- Implement replacements for legacy services, with emphasis on efficiency, security, and reliability.
- Devise technical, social and political solutions for compliance with industry regulations.
- Conduct feasibility studies and pilot programs for potential implementations.
- Present findings to business owners, managers and technical leads.

Platforms

- **Linux**: SLES, OpenSUSE, RedHat, RHEL, Fedora, Mandrake, CentOS, Ubuntu, Backtrack, Debian, Knoppix, Slackware
- **Microsoft**: DOS 3.3 – 6.2, Windows 3.1, 95, 98, NT, ME, 2000, and XP, 2000, 2003, 2008
- **Unix**: Solaris, SCO OpenServer, FreeBSD, OpenBSD, NetBSD, OSX, HP/UX, Irix, TRU64
- **Other**: Mac Classic, Cisco IOS, PalmOS, OpenVMS
- **Web**: Google Apps, Mediawiki, Joomla, Wordpress, Drupal

Security Tools

- **Unified Threat Management**: Fortinet, Astaro, Watchguard, CheckPoint, Barrier1, Cisco, IPCop
- **Web Protection**: Imperva, CloudFlare, Sophos UTM, mod_security2, php-suhosin, Apache2, IIS
- **Managed Services**: Alert Logic, Solutionary Activeguard, Google Message Security, ShadowServer Alerting
- **Endpoint Protection**: Sophos, Bit9, Safeguard, Symantec, ClamAV, iptables, tcpwrappers, AppArmor
- **Network Assessment**: Nessus, OpenVAS, Core Impact, nmap, kismet, metasploit, Zenmap, ExploitDB
- **Monitoring**: mon, n-able, monit, nagios, collectd, tcpdump, ethereal, wireshark
- **Public Analysis**: Paterva Maltego, SearchDiggity, pipl.com, snoopstation, many custom scripts
- **Private Analysis**: John the Ripper, Ophcrack, CheckRootKit, RKhunter, Exiftool
- **Web Assessment**: Burpsuite, NetSparker, nikto, Rat Proxy, Skipfish, Accunetix

Software

- **Web**: Apache 1.3.x-2.x, mod_perl, PHP, ruby, mongrel_cluster, squid, Tomcat/J2EE
- **Web Systems**:, Gallery, eWiki, Twiki, SugarCRM, dotProject, dokuwiki
- **Email Systems**: Qmail, GroupWise, Vpopmail, Squirrelmail, Courier IMAP, ezmlm, Sendmail, Postfix
- **Database Services**: PostgreSQL, MySQL, Berkley DB, SQL Relay
- **File Services**: ProFTPd, Vsftpd, NFS, samba, Novell file services
- **System Administration**: OpenSSH, NFS, cron, subversion, VNC, CUPS, OpenLDAP, yum, eDirectory
- **Web Clients**: Firefox, Mozilla / Netscape, Firefox, Opera, Internet Explorer, elinks, w3m, telnet
- **Graphic**: Gimp, Inkscape, Bibble, ImageMagick, PaintshopPro, Photoshop, POVray, Ghostscript/PCL
- **Backup Tools**: SyncSort Backup Express, amanda, LoneTar, bacula, tar, zip, bzip, gzip
- **Virtualization**: VMWare, VirtualBox, Xen, Solaris Containers/Zones

Languages

- **Scripting**: Perl, Unix Shell, Javascript, PHP, Ruby, Python, SQL, Expect, DCL, Windows Batch
- **Compiled**: C, C++, Java, Scheme, Pascal, Fortran, Basic, POVray, Logo
- **Descriptive**: HTML, DHTML, XHTML, XML, CSS, YAML, TEX

Networking Protocols

- **Standard**: HTTP, FTP, SMTP, Telnet, TCP/IP, POP3, IMAP, NTP, DNS, IRC, SMB
- **Secured**: HTTPS, FTPS, IPsec, SSH, IMAPS, POP3S

Data Sources

- **Industries**: Municipalities, Banks, Credit Unions, Utilities, Medical, Development, Collections, Health Care, Trucking, Insurance, Nonprofits, Political Parties, Retail, Manufacturing, Retirement, Software, Publishing, Distributing, Utilities
- **Formats**: Delimited, Mainframe extractions, IBM and AS400 spools, Word, Excel, Access, DBase, Foxpro, PDF, Postscript, PCL, XML, Raster graphics, Mailspools