Spicer Conant

San Marcos • CA • spicer@conant.org • www.conant.org • 714-357-7768

Operational Risk Consultant / Operational Security Manager

Highlights

- Global banking experience in Risk Management / Security / Governance / Compliance / Audit
- Detail-oriented, security-focused, process-based Information Systems Engineer and IT Auditor
- Professional, communicative, procedural, highly-organized and Team player

Experience

Ernst & Young, LLP (Financial risk / Cybersecurity)

Consulting Manager FSO Advisory / ITRA Group -- Irvine, CA 09/2015 to 08/2016

Risk Management / Cybersecurity
Cybersecurity and data analytics for large financial institutions. Conducted IT risk analysis / IT external audits using EY audit tools. Created metric-based reports and consulting decks for both internal and Client-facing projects and proposals. Worked with various datasets to mine for pertinent metrics and provide meaningful analytics. Conducted Cybersecurity audits / Cyberthreat analyses in the financial sector.

Wells Fargo Bank & Co. (8+ years Financial industry)

Technology Manager Wells Fargo Bank – San Marcos, CA 03/2012 to 06/2015

IT Audit / Operational Risk Management
Performed internal IT infrastructure audits on Windows Server 2003 and 2008 R2 machines. Applied COBIT 4.1 and 5 framework control objectives to the systems and servers to maintain Sarbanes-Oxley (SOX) financial industry compliance. Verified compliance with US Government-mandated document retention policies. Performed server-based information systems security analyses and internal first-level penetration testing (full-scale pen testing was outsourced). Used several of the COSO internal controls to ensure system uptime and provide feedback for Stakeholders (primarily risk assessment and system monitoring controls). Reviewed user configuration access per bank-wide access control and governance policies. Reviewed external (Wholesale Bank) IT Security Audits to ensure hardened system security & compliance with both bank and Government standards (NIST and ISO). Implemented change controls and performed change management using the internal PAC2000 system of record. Data Transmissions Team engineering liaison to various Agile scrum teams for software development and deployment.

Hands-on Systems Engineering
Managed and configured secure data transmissions environment (my group was responsible for inbound and outbound LOB wires totaling over $1 billion daily). Implemented application and server baseline compliance. Conducted Windows event log audits and reporting. Configured and supported user access controls (IDM) to secure and monitor encrypted transmissions environment. Wrote complex scripts for various data transmissions processes (file send/receive, system maintenance, system security audit, lockout controls, alerting and system monitoring). Supported Secure File Transfer (proprietary SFT system built internally by WF). Implemented and conducted pro-forma security audits on Sterling Commerce / IBM NDM Connect:Direct systems (point-to-point secure connections over SSL/TLS certificates). Configured server-side SFTP (SSH FTP / Secure FTP) and FTPS (FTP over SSL) for high-volume secure data transmissions.

Personnel Management
Data Transmissions Group Technical Manager (Player/Coach hands-on leader). Managed a group of 5 engineers distributed throughout the US (Los Angeles, New York, Minneapolis, Charlotte). Performed EOY personnel reviews and created baseline Management-by-Objective (MBO) goals for individual contributors. Maintained current user rights assignment and security group membership via authorization and approvals.

Business Systems Consultant Wells Fargo Bank - Santa Monica, CA 06/2010 to 03/2012

Operational Risk Management
Implemented SDLC (Software Development Life Cycle) reviews for new and existing data transmissions systems. Conducted internal security and systems audit remediation and compliance for Windows Server implementations. Developed and analyzed TCO calculations for remote training systems. Conducted internal NDM application audits for preventative and detective access controls to harden and restrict access to QA, DEV, BCP, pre-PROD and PROD systems. Reported gaps in systems per the COBIT governance model (adhering to both internal and external compliance standards). Worked directly with LOB ISO (Information Security Officer) to maintain the ISO-27001 and ISO-9001 certification. Acted as the Team Data Assurance Manager for BCP (Business Continuity Planning) and DR (Disaster Recovery).

Hands-on Systems Engineering
Designed and supported Windows Server Infrastructure. Performed Windows server event archiving, auditing and scheduled task maintenance. Interfaced with other national and international banks in support of data transmissions, risk and compliance. Configured and executed Business Continuity Planning (BCP testing and analyses) using VMWare virtualization. Used VMWare SMVI (Snap Manager for Virtual Infrastructure) on ESX hosts to replicate real-time data from primary Santa Monica data center to redundant Boston hot site. Setup FDE (Full-disk Encryption) on client devices. Verified IDS (Intrusion Detection System) on critical LOB servers. Developed and maintained CLI server scripts for IPSwitch FTP.

ID Management / Compliance
Implemented User Management and security group access controls. Created an IDM approval process for the Wells Fargo / Wachovia merger. Wrote PnP (Policy and Procedure) documents for the WF / WB merger. Verified cross-functionality SSO (Single Sign-on) and FIDM (Federated ID Management) user setup on multiple systems in a heterogeneous application environment.

Server Engineer Wells Fargo Bank - Santa Monica, CA 02/2008 to 06/2010

Server Systems Engineering & Security
Developed on-site and remote Windows-based production client/server architecture, configuration and implementation. Designed, deployed and supported a mobile training center architecture for merger-related cross-platform training sessions. Supported server management and security configuration via SCOM. Audited, documented and presented local ActiveDirectory policy application and enforcement (server-side). Performed server builds per internal specifications. Configured implementations of various in-house interfaces (ART, SAFE-T, OracleGL, BASEL, OFAC, MCV, OneGL, CIS and MRA). Installed and configured rack-mounted server hardware / OS / applications on pre-PROD and Production LOB servers. On-site system support (San Francisco, Boston, Chicago, New York).

Compliance and Risk Management
Implemented COSO control remediation steps per internal audit (Windows Server policies, NDM, SAFE-T). Followed internal and external guidelines for security policy and asset management. Implemented policy guidelines and/or recommendations (using post-audit remediation goals generated). Reviewed and documented risk levels calculated for Production systems.

LEHREN Systems, LLC (10+ years technical TV & Film industry)

Security Operations Manager LEHREN Systems - Los Angeles, CA 05/2005 to 05/2007

Infrastructure Security / Digital Rights Management (DRM) / Compliance
Verified role-based access control using AD and stand-alone authentication (group model). Supported DRM (Digital Rights Management) system to protect proprietary Customer content. Configured physical and logical security for all hardware and software systems that were provided to the Customers. Verified the hardening of servers via host-based IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) tools. Restricted access to clients and servers using role-based access methodologies. Responsible for maintaining and documenting FCC compliance.

Hands-on Systems Engineering
Designed, engineered and supported mobile TV graphics systems for sporting event production. Developed ActiveDirectory configuration Windows Server 2003 (pre- and post-Production environments). Supplied client and server hardware and software systems (viz|rt, Trio) for live, direct-to-air proprietary computer graphics content (customers included ESPN, ABC, CBS, DirecTV, and NFL Network). Conducted onsite and remote technical support for live sporting events. Designed and supported Windows Server security lockdown via Active Directory GPOs. Managed OSSEC and Snort HIDS systems (monitoring & alerting).

Personnel Management
Hands-on Manager: acted as the Team Lead for a group sub-contractors on various projects.

IT Infrastructure Engineer LEHREN Systems - Munich, DE 06/2003 to 03/2005

CMS / DRM / Security
Developed server-side security models for the German Act for Telecommunications Media Services (Telemediengesetz, preliminary preparation prior to enforcement of official Government regulations). Installed and configured Blue Order Media Archive. Setup AVID video servers (applying security controls and audit measures to ensure restriction of access). Reviewed DVB Content Protection and Copy Management (DVB-CPCM) governance policies using portions of ITSEC (Common Criteria). Performed security control gap analyses on server-side CMS for 200,000-clip video library running on 10PB SGI array.

Active Directory Architecture & Systems Engineering
Systems Engineer and Technical Operations Manager for TV Production environments. Architected and implemented complete Windows Server Active Directory domain for new all-digital broadcasting complex (German television). Developed and implemented ActiveDirectory security groups hierarchy. Performed IT Management and technical support for server-side computing. Was the primary Technical Project Manager for the Freimanner Sendezentrum ActiveDirectory installation. Maintained European Union (EU) broadcast, audit and compliance standards and regulations.

Exchange Messaging Architect LEHREN Systems - Munich, DE 01/2000 to 06/2003

Microsoft Exchange Architect / Implementation Engineer
Designed, implemented and supported the Microsoft Exchange multi-site environment for company-wide Exchange initiative. Performed server rollout, configuration and security policy management for 20 server / 1000 client Exchange mesh. Conducted backup and restore administration using Legato Networker (using both SCSI disk arrays and tape jukeboxes for backup & retention systems).

Technical Production Manager for Remote TV Productions
IT infrastructure design, implementation and support for remote television productions:

- ARD Remote Studio IT Security / Infrastructure Design / Implementation (Israel and Austria)
- ARD / ZDF Ski World Championships (St. Moritz, Switzerland)
- 2002 European Track & Field Championships (Munich, Germany)
- 2002 Winter Olympic Games (Salt Lake City, USA)

Systems Engineer LEHREN Systems - Munich, DE 09/1997 to 01/2000

Windows Server Builds & Engineering
Primary MCSE for the company-wide Windows NT Server 4.0 and Windows 2000 Server rollout (both diskless using bootp and via TCP/IP custom boot floppies). Designed the NT Security Account Management (SAM) configuration using both local "stand-alone" and WinNT Domain models. Built and maintained server hardware (primarily Compaq / HP multi-core servers) as well as OS installation and configuration.

Technical Documentation & Presentations
Created AutoCAD and Visio server architecture documentation (Domain maps). Wrote End-User training manuals to accompany the Client rollouts. Presented upgrade path and hardware/software sunset roadmap and trajectory plans to various levels of Executive Management (live presentations conducted in German).

Scripps Institution of Oceanography (3 years Science & Research industry)

Data Analyst Scripps Institution of Oceanography (SIO) - La Jolla, CA 02/1993 to 06/1996

Database Admin
Constructed and managed proprietary online database called the DataZoo at CCS / SIO. (NOTE: initially funded by the US Government MMS project, the idea of putting public domain data online in an HTML / hypertext format was at the time very cutting-edge and well received). Maintained the database user access structure. Configured internal and external access routes (HTTP, FTP, Gopher and Lynx).

ID Management
Maintained network user rights management systems and end user access control policies. Setup and managed FTP users on Sun SPARC / SunOS / Solaris UNIX servers. Configured NFS mount points and user access controls to disk arrays. Created server and workstation network users and managed access to databases and network shares.

Technologies Overview

Platforms
Hardware: x86, RISC (PPC), MIPS, ThinClient (diskless workstations), Dell servers, Compaq/HP servers, bare-metal blade servers (various models), clusters and HA-servers, ESX hosts (VMWare).

Operating Systems: DOS, all Windows platforms starting with Win 3.11 (Workgroups), Win95/98, WinNT3.51/4.0/TSE/W2K0/WinXP/PE/W2K3/2003/2008 and 2008R2/Win7/8, UNIX (SunOS/Solaris), Linux, Irix, Android (Cupcake through Lollipop), MacOS, OSX.

Software & Systems
NDM (IBM Sterling Commerce Connect:Direct Network Data Mover), command-line SMTP email scripting (blat / sendmail), SSL/TLS certificate implementation, Exchange Server (4, 5.5, 2K0, 2K3), all Microsoft Office Suites, Photoshop, bit / block-level file and OS replication (data mirroring), vi, Eudora, Linux (RedHat, SuSE), VMWare vCenter SMVI / SnapMirror, Snort, web server development tools, HTML3/4/5, JavaScript, jQuery, CSS3, sysprep / cloning and systems rollout (Ghost, IC3, ImagePro), unattended setup and rollout via OMA (Linux) and NetInstall, Hexdump PowerShell scriptlet (0x16e), Legato NetWorker backup and restore (Exchange and Oracle), packet sniffers and network monitors, various Networking utilities, symmetric and asymmetric encryption configurations, Sysinternals PS-tools, PGP / GPG, WindowsPE rollout (BartPE and UBCD), SQL database mirroring, VPC (Oracle VBox, MS VPC), OSSEC, WAN file replication and synchronization, CMS (Content Management Systems), various PKI systems (stand-alone and CA-based).

Networking
Topologies LAN/WAN, Ethernet over copper / Wi-Fi / fiber (CSMA/CD and CA), Token Ring 4/16, Demand Priority, ATM, iSCSI.

Protocols IPv4/6, TCP/IP, NetBEUI, IPX/SPX, DLC, PPP, PPTP, SLIP, AppleTalk. Heterogeneous management of server-based and peer-to-peer LAN (LDAP, SAM, Active Directory, NDS, Unix, Linux integration). RADIUS server, VPN (L2TP and PPTP), email host/gateway configuration and maintenance.

Computer Based Training
Developed and conducted proprietary on-site email training classes for Customer Service Representatives (wrote all training manuals). Conducted server-based computing (ThinClient) training for both technical groups and Executive Management.

Formal Education

BA Cognitive Psychology/Human-Computer Interaction (UC San Diego)	06/1996
European Foreign Exchange (University of Sheffield, England)	06/1995

Continuing Education

CISSP (ISC^2 Certified Information Systems Security Professional #507488)	02/2015
Wells Fargo Risk and Compliance / OFAC (Foreign Assets Control)	03/2009
Cisco VPN & IOS Administration (Site-to-Site VPN Admin)	01/2008
Windows Server Active Directory Design & Architecture	03/2005
OMA (Certified Open Management Architecture Administrator)	06/2004
NetSupport / NetInstall Software Distribution Administrator	07/2001
Certified Legato Networker Backup Administrator	06/2000
Microsoft Office Suite Certificate (MVHS, Munich)	03/1999
MCT (Microsoft Certified Trainer)	08/1998
MCSE (Microsoft Certified Systems Engineer)	07/1997
CNS (Certified Network Specialist, UCSD)	03/1997
MCP / MCPS (Microsoft Certified Professional #379652)	12/1996

Awards and Interests

Languages: English mother tongue, fluent German (reading / writing / speaking), basic Spanish
Global work experience: United States, Mexico, Europe, Middle East, China, Australia
Provost Honors (University of California, San Diego)
Long-distance bicycle tours (Europe, Americas)
Avid backpacker & long-distance bicycle rider
Advanced Open Water scuba diver
Whitewater Kayak Instructor
Eagle Scout