**Brian A. Mitchell**

**16606 Eldbridge Ln**

**Bowie, Maryland 20716**

**Brian.Mitchell2006@gmail.com**

**(301) 395-3235**

**EXECUTIVE PROFILE**

**Chief Information Officer-Chief Technology Officer-Director of Information Technology**

**Chief Information Security Officer- Director of Information Security**

|  |  |
| --- | --- |
| * Cloud Consultant for AWS | * Program & Project Management |
| * Budget & Cost Control Delivery | * Staff Development, Mentoring & Hiring |
| * Leadership & Management Training | * On-site & Off-Shore Managed Services Delivery |
| * Governance Risk & Compliance with Auditing | * AD & Identity Access Management Design |
| * Technology Architecture & Integration | * Contract Negotiation & Development |
| * Direct and Indirect Employee management | * Strategic Analysis & Internal Consulting |

**Leadership Experience Abstract**

Throughout my professional career, I have excelled in all areas of Information Technology within the federal government and the private industry. I’ve had the pleasure to serve on executive steering committees focused on strategic planning, P&L responsibility and profitability improvements along with budgeting & finance initiatives set forth by the Secretary of Treasury and the Administrator of the U.S. Small Business Administration. With over 18 + years of knowledge devoted to performance optimization of large scale enterprises coupled with exemplary executive managerial efficiency has afforded me the opportunity to support and help many organizations reach their goals.

**Select Accomplishments and Achievements**

* Developed and led the creation of the U.S. Small Business Administration Security Operation Center (SOC), where I assisted the CISO in establishing roles, policies and procedures.
* Received an achievement reward from the CIO for helping save $400.000 dollars in cabling cost and $1.5 million in new equipment purchases by deferring upgrading to CAT 6 vs CAT 5e from CAT 3.
* Delivered Good Technology SAAS Mobile Device Management (MDM) solution, which saved over $2.4 million on budgeted new purchase orders for the “Bring your own device” (BYOD) initiative.
* Successfully implemented cloud security for Big Data encryption between SBA’s headquarters, datacenters and financial banking institutions.

**SKILLS**

Security Cloud Advisor, Network & Security Cloud Architect Design, Program & Project Management, Network & Security Operations Management, Executive Steering Committee Technical Lead & Presenter, CONOPS Development, Staff Development, Contract Negotiation & Procurement, Budget & Cost Control Delivery, Datacenter Construction & Development, Governance Risk & Compliance. Executive Decision-Making & Best Practices with Benchmarking and COOP Development & Training agency-wide along with local & state governments.

**PROFESSIONAL EXPERIENCE**

**AMTechnology LLC. (40 hours) Nov. 2016 – Present**

**Client Department of Energy, Washington DC/Germantown MD (On-Premise)**

**Client ITSourceTek Inc, San Rafael, CA (100% Remote)**

**Client Fort Washington Medical Center, Fort Washington, MD (On-Call, On-Premise & Remote)**

**Client United Airlines, Chicago, IL (On-Premise)**

**Client Purisolve Inc/Dept of Treasury, New Carrollton, MD (IRS) (100% remote)**

**Client Trilogy Education Services, New York, NYC (On-Premise & Remote)**

**Client Mercantil Commerce Bank, Miami, Florida (On-Premise & Remote)**

**Director of Information Security, Information Manager, Senior Security Architect and Cloud Security Strategist (Consultant)**

* Developed Security Operation Procedures for the IM30 group base on NIST 800-61 r2 for DOE.
* Developed and implemented strategies to monitor and comply to the ongoing Security Operation Center changes in day to day ticket request for DOE.
* Coordinate and review ITSourceTek client requirements and provide strategic planning and technical guidance to ensure performance optimization in order to achieve the organizational goals.
* Consultant with ITSourceTek executive management regarding client strategies and security product joint ventures & alliances to better serve the CEO, EVP and CIO profitability goals for the company.
* Deliver and coordinate all new business development opportunities to ITSourceTek CEO in order to secure contractual agreements for new products and services.
* Consultant with Fort Washington Medical Center CEO, COO and CIO on Information Technology Health requirements and implementation of new policies and procedures aligned with new hospital development projects which require compliance regulations, statues and accreditation requirements for (HIPAA, EMTALA, CMS Conditions of Participation, DNV/Joint Commission, NIAHO and ISO 9001)
* Actively addresses and advises the Fort Washington Medical Center CEO on changing healthcare IT infrastructure concerns and proposes new security measures to ensure complete protection of patient information.
* Led a team of subject matter expert engineers in the implementation and use of Oracle’s Identity Cloud Service to work with United Airlines Sun Identity Manager/Oracle Waveset on-premise solution.
* Delivered a comprehensive phased road map approach for building a Security Transit (Virtual Private Cloud) VPC on AWS at United Airlines (UAL)
* Consulted with all departments of UAL on security measures for the cloud across multiple cloud provider platforms explaining how their information would securely be protected.
* Collaborated and influenced senior executives on tool selections for the use in the cloud security architect design within United Airlines.
* Supported the initiative for the implementation of IBM BigFix and RESOne through team meetings and workshops with the Internal Revenue Service (IRS).
* Oversaw research and development of the IRS infrastructure working in a BigFix environment virtually before deployment into production.
* Developed one on one meetings with team members for status updates and progression metrics to keep IRS upper management abreast on the implementation efforts.
* Worked within a team cohesively to complete IRS qualifications standards dealing with different toolsets for which we needed to be proficient in.
* Designed network architect for Trilogy Education Services in the development of the first intranet linking, New York, NY, Boca Raton, FL and Tempe, AZ comprised of cisco routers and switches along with Microsoft Servers 2016, SCVMM, and MS SCCM for Windows 10 deployments.
* Developed mitigation strategy with engineers to implement Office 365 and Azure Active Directory premium service combined with Microsoft Identity Access Management within Trilogy Education Services.
* Created mitigation strategies with Microsoft subject matter expert engineers to implement Salesforce with Azure API Apps connection within Trilogy Education Services.
* Devised and proposed an internal security plan developed from NIST Publication 800-53 rev 4 for Trilogy Education Services.
* Established and proposed internal disaster recovery plans tied into daily and weekly maintenance to the cloud and datacenter for Trilogy Education Services.
* Developed and gathered metrics on the network & security infrastructure to present to the CEO and COO of Trilogy Education Services.
* Managed and mentored a team of 15 Mercantil banking security engineers on daily metric gathering to present to the banks senior executive staff bi-weekly.
* Accepted ownership for the strategic redevelopment of the Mercantil network “Change Management” process, by developing roadmaps, use cases and KPI’s in order to strengthen the process.
* Oversaw and managed Mercantil budget for the purchasing of 3rd party certificates from Venafi.
* Managed Mercantil operational budgetary cost from the implementation projects of Database Access Management (DAM) and File Access Management (FAM) in accordance with the Federal Financial Institutions Examination Council (FFIEC) and the Office of the Comptroller of the Currency (OCC).
* Directed Mercantil security team that monitored and administered changes within SailPoint for Identity Access Management.
* Oversaw the outsourcing negotiations, budgeting and contract signing for managed services in support of Tier 1 & 2 for Mercantil.
* Managed Mercantil negotiation of contracts for penetration testing which was awarded and administered by Rapid 7 in the areas of wireless security, social engineering and network penetration.

**Wipro Technologies (40 hours) Oct 2015 – Nov 2016**

**Client McClatchy Inc, Miami, Florida (On-Premise & Remote)**

**Client Vantiv Inc, Symmes, Ohio (On-Premise & Remote)**

**Client Catholic Health Initiative, Englewood, CO (On-Premise & Remote)**

**Client Hanesbrands Inc, Winston Salem, NC (100% Remote)**

**Director of Information Security, Senior Program Manager and CYBER-SOC Manager**

* Managed and trained 5 onsite and 30 offshore employees for 24/7 Tier 2 & 3 coverage for monitoring services of cloud security, vulnerability scanning, threat intelligence, wireless network security, and security patching.
* Managed and trained 5 onsite and 30 offshore employees for 24/7 Tier 1, 2 & 3 coverage of all Microsoft Windows Servers with Hypervisor, SCVMM, Exchange, SharePoint, Windows Desktop & Laptops. Also, VMware VCenter, including Linux operating systems and Unix (AIX) servers. Including all data backing up on EMC^2, Oracle and into the Cloud Storage servers.
* Developed and gathered network & security infrastructure metrics to present to CEO, COO, CFO and CIO.
* Created strategic transition modules to ensure accurate knowledge gathering and transferring from managed services of enterprise network security, AWS infrastructure as a Service (IAAS) and AWS Cloud storage.
* Managed multiple environmental changes from the purchase of multiple companies consolidated under one umbrella administrated by Identity Access Management and Active Directory platforms.
* Led a team of subject matter experts in the implementation and knowledge transfer of Symantec VIP for two factor authentication and Symantec Identity Access Manager (SAM) for McClatchy.
* Managed and monitored several senior leads on the knowledge transfer of employees being RIF, while hiring and recruiting new resources needed for the engagement from France, India, Kentucky and South Florida for McClatchy.
* Led a team of SME’s to take over all Microsoft Server 2012 SCVMM, SCCM, Linux Servers, Unix (AIX) Servers, Load Balancers, Cisco Routers and Switches, SIEM, Vulnerability Scanner, Symantec Endpoint Protection, Symantec VIP
* Advised and supported the development of an Information Security Plan using NIST 800-53 Rev 4, to solidify standards for security the network infrastructure.
* Led a team of SME’s to consolidate and architect the combining of 32 active directory forest into 1 forest with trees, using Active Directory Migration Tool (ADMT).
* Managed and created a charter for the Vulnerability Assessment Team (VAT) weekly, monthly and quarterly reporting on all non-compliant devices on the network, DMZ and cloud business devices using PCI.
* Led a team of subject manager experts to explore expanding CA Technologies solutions for PCI compliance and IAM within Vantiv to newly acquired companies in order to eliminate waste.
* Oversaw the gathering of documentation related to PCI and SOX requirements for McClatchy, in which the CIO and CFO had to give their verification via signature that they network credit card information was protected.
* Delivered IBM’s BigFix Endpoint Manger Solution to over 5,000 server endpoints with an additional 10,000 endpoints comprised of laptops, PC’s and tablets for Vantiv Inc.
* Managed a team of 25 direct reports, 35 indirect reports and 50 overseas employees for Catholic Health Initiatives CYBER-SOC for 24/7 monitoring of Tier 2 and 3 ticket requests.
* Oversaw and managed the Catholic Health Initiatives managed CYBER-SOC expanding over 104 hospitals and 30 plus clinics nationwide.
* Developed and created Catholic Health Initiatives policy and procedures derived from compliance regulations, statues and accreditation requirements for (HIPAA, EMTALA, CMS Conditions of Participation, DNV/Joint Commission, NIAHO and ISO 9001)
* Oversaw and worked with medical staff in review of all policies and procedures delivered for review during our Medical Executive Committee (MEC) concerning security issues for Catholic Health Initiatives.
* Managed and developed policy and procedures for Hanesbrands Inc CYBER-SOC with increase threat monitoring and increasing threat response timing.
* Managed a team of 15 direct reports, 20 indirect reports and 25 overseas employees for Hanesbrands Inc CYBER-SOC for 24/7 monitoring of Tier 2 and 3 ticket requests.

**U.S. Small Business Administration (SBA) (40 hours) Apr 2014 – July 2015**

**Office of the Chief Technology Officer, Washington DC**

**NOC Manager/Acting Chief Technology Officer (CTO)/Subject Mater Expert (SME)**

* Assisted in managing 160 employees comprised of Network Engineers/Architects, System Administrators/Analyst, Security Analyst/Engineers, Database Engineers, Program/Project Managers and Lead Technical Analyst/Engineers.
* Provide the Chief Technical Officer (CTO) with technical leadership and guidance on agency-wide

strategic IT planning implementations.

* Provided direct tech support and organizational leadership within the weekly Change Management Meetings geared to improve the overall service level and capacity management of Tier 1, 2 and 3 employees.
* Effectively implemented risk and cost saving measures to neutralize known network security gaps within the intranet and demilitarized zone (DMZ).
* Provided leadership to subject matter experts comprised of tiger teams in order to combat special needs of the SBA network infrastructure.
* Delivered structure and knowledge to smaller divisions within the agency utilizing AWS GovCloud services to host internal websites and backup local data.
* Provided executive technical advisory, strategic planning, coaching of staff and mentorship of team members on organization and agency-wide directives to better understand the mission.
* Developed IT strategy for the documentation and signing of Request for Comments (RFCs) for new or preexisting server projects through the Control Change Board (CCB) and Enterprise Change Control Board (ECCB).
* Provided weekly budgeting & finance metrics on multi-site operational projects for senior management.
* Effectively implemented risk and cost saving measures to neutralize network security gaps within our intranet and demilitarized zone (DMZ), which prevented the leak of government secure information to the public.
* Worked with and supported Tier 1 Helpdesk Analyst and Tier 2 & 3 NOC Engineers to build/refresh Domain Controllers throughout the agency. This was accomplished by building new Domain Controllers on Dell T610 and R610 servers, loading Microsoft Server 2012 r2 along with the configuration for the DC in the operating system. Loading and creating a standard image for all machines while joining and prevising them to the network before shipping them out.
* Worked on the implementation to install/upgrade SCVMM from 2008 to 2012 for all windows servers 2008 to 2012.

**U.S. Small Business Administration (SBA) (40 hours) Apr 2008 – Apr 2014**

**Office of the Chief Information Officer,**

**Chief Information Security Officer, Washington DC**

**Cyber-SOC Manager/Vulnerability Manager/Program Manager & Acting CISO**

* Managed 43 contractor employees comprised of Network & Security Administrators/Analysts and Engineers.
* Developed and gathered network & security infrastructure metrics to present to senior executive during the bi-weekly steering committee.
* Directed the certification and accreditation activities (C&A) for audit support with KPMG reviews and improvement development of the Security Operation Center (SOC).
* Established and improved the SOC security system reporting and monitoring capabilities from FY 2011 to FY 2012.
* Provided critical leadership, guidance and approval of all C&A, Plan of Action and Milestone (POAM) in order to help certify the agency’s information technology systems regulated by NIST and FISMA controls.
* Acted on behalf of the CISO for all voting matters related to security of the network during the Enterprise Change Control Board (ECCB) meetings.
* Directed and managed the Vulnerability Assessment and Testing (VAT) team dedicated to the removal or repair of security vulnerabilities on the network using Nessus & McAfee Foundstone and automated patching with IBM’s BigFix solution.
* Oversaw and worked hands-on with FedRAMP requirements for the security architect design for AWS GovCloud.
* Led the agency-wide Citrix upgrade and XenDesktop 7.5 deployment contract which supported the

implementation of the Telework Enhancement Act of 2010 signed by President Barak Obama.

* I created and developed policy and procedures in the establishment of SBA’s first Security Operation Center (SOC), where I assisted the CISO in job description creation along with hiring of staff.
* Oversaw the development of the SOC into a CYBER-SOC moving from multiple shift overlapping at different times during a 12 hour period to a 24/7 work schedule.
* Led the implementation and upgrade of the firewall from Cisco ASA to Checkpoint, along with the upgrade from McAfee Foundstone to Nessus Vulnerability Scanner built on top of Linux.
* Purchased the agencies first VMware software license and developed the Security Operation Center VMWare VCenter server platform to load the security tools as Virtual Machines running on “Centos (Linux)” OS.
* Oversaw the development of the SOC into a CYBER-SOC moving from multiple shift overlapping at different times during a 12 hour period to a 24/7 work schedule.
* Developed a Virtual SBA Network which was connected between the Helpdesk, NOC and SOC. Access was controlled by two Cisco ASA Firewalls in which the helpdesk used to join new computers to the network, windows, linux, IOS etc.. along with the NOC added new server images and converted physical servers using VM Converter or P2V to test the VM workloads. Next Security scanned and tested vulnerabilities and baseline. McAfee EPO was pushed out to the devices and once everything was fully tested, these devices was taken to the change control board to be approved for production deployment.
* Worked on the implementation upgrade and control from the NOC to the SOC of Microsoft Identity Lifecycle Manager 2007 to Microsoft Forefront Identity Manager 2010 R2 Service Pack 1.

**U.S. Small Business Administration (SBA) (40 hours) Apr 2006 – Apr 2008**

**Office of the Chief Information Officer,**

**Chief Information Security Officer, Washington DC**

**Helpdesk Analyst /NOC Lead Engineer/Exchange Manager/Storage Manager**

* Worked on the helpdesk for 6 months as part of my network operations training, troubleshooting tickets, reimaging desktops, laptops. Securing Laptops with Safe boot encryption,
* Worked on the helpdesk, adding new users to Active Directory OU’s, adding printers’ connections to their desktops, remotely logging in to fix issues with share drives and anything else they had issues with.
* Worked as a NOC Engineer and was later promoted to a NOC Lead, where I was confirming cisco routers and switches, creating VLANS, working with the helpdesk to troubleshoot connection issues from the switch and patch panel all the way to the user’s desktop.
* Worked with Windows Server 2003 and the implementation upgrade to WS 2008 R2, with Hypervisor and SCVMM 2008 on Dell Server Blades utilizing EMC^2 storage.
* Worked with Oracle, Microsoft SQL Server and Symantec/Veritas backup exec for all SAN, NAS and DAS connected to the SCVMM. All data was storage locally and then offloaded to Iron Mountain and tested during our DR and COOP controlled exercises.
* Worked on the implementation of Windows XP to Windows 7 upgrade, creating images and sending them out to the field engineers, along with working remotely to facilitate the upgrades with user’s information being transferred to local network storage.
* Worked as the exchange administrator creating mailboxes for new employees and organizations needing public mailboxes. Along with deleting, archiving mailboxes of retired employees or those leaving the agency and reconnecting that mailbox to their managers outlook. Login into user’s outlook and adding out of office messages on and forwarding mail to a designated group mailbox.
* Worked on the blackberry server implementation as the exchange administrator, syncing and making sure the mail was updating the blackberry server at the same time.
* Worked on the SharePoint implementation for creating the interoffice sites and served as the administrator over the sites and gave access to local site administrators to update content for their organization.
* Worked on the Active Director forest raised project from 2003 to 2008, for the new Windows Server 2008 r2.
* Worked with the implementation of Citrix Xendesktop servers in order to allow SBA employees to access a image of their desktop remotely in case they didn’t have a mobile laptop during an emergency, for example the times when the government was shut down. Employees who were telework ready were able to work remotely and I worked to make sure this happened.
* Worked on the implementation upgrade of Microsoft Identity Integration Server 2003 Enterprise Edition to Microsoft Identity Lifecycle Manager 2007.

**U.S. Department of Treasury/Internal Revenue Service (IRS) (40 hours) Jun 2000 – Apr 2006**

**Compliance Systems Division, New Carrollton, Maryland**

**IT Specialist/Program Manager/Computer Programmer**

* Provided strategic planning, financial and network implementation updates for senior executives during weekly or bi-weekly steering committees.
* Developed and launched the Tax Exempt and Government Entities (TEGE) database to gather and track funds owed by organization to TEGE.
* Controlled and facilitated status meetings with senior management and contractor staff on network issues arising during tax season for the Final Integration and Testing (FIT) organization.
* Maintained and administered the tracking of Customer Account Data Engine (CADE) which was developed by CSC to ensure systems software and databases for defect resolutions and implementation efforts carried out by both IRS employees and CSC Contractor employees.
* Provided daily and weekly updates of funds and funding in detailed reports, which were carried out and managed throughout the division for future requisitions for budget proposals.
* Provided technical support and implemented new domain and server connections on the Sun Solaris E10K and E15K enterprising network servers.
* Conceived and reengineered Cobol programs to manage US citizens tax returns within the IRS environment during production and testing phases throughout the fiscal year.

**AllFirst Bank/M&T Bank (40 hours) Jan 1998 – June 2000**

**Oxon Hill, Maryland**

**Bank Manager/IT Helpdesk Associate**

* Coordinated with customers and Branch leadership to schedule financial investment appointments and meetings to discuss investment opportunities and to present proposals for promotional consideration to the Branch leadership.
* Oversaw the daily operations of Branch activities, which includes managing and ensuring proper training and development of a staff of 8 banking professionals.
* Performed a wide range of administrative duties, including scheduling appointments, preparing correspondence/briefings for conducting research and fact finding.
* Trained and advised all employees on my expectations for the branch during daily operations and work with each of them to leverage their professional talents and expertise to further the goals and objectives of the branch.
* Oversaw and coordinate the development and implementation of a financial management campaign to facilitate the acquisition of more revenue and deposits into the branch.
* Worked with and answered phone calls dealing with computer related issues within the bank.
* Worked a weekend shift in the IT helpdesk call center in support of internal employees and external customers computing needs.

**Core Competencies**

Cloud Security, Cloud Migration to IaaS, VMware and Hyper-V Virtualization, Enterprise IT Architecture, Business Intelligence, Cloud Storage and Big Data, Wireless Network Security, Windows Desktop Support

**Platforms:** UNIX (Solaris), Centos (Linux) 4, 5, 6.5, 7.5, MS Windows 95/98/NT/XP/Vista/Win 7/

Win 8.0-8.1/Win 10, Server 2000, 2003, 2008R2 with Hyper-V, 2012, 2016 standard & enterprise

VMWare player, workstation, vsphere 3.1, 4.1, 5.0 and 5.5, Citrix XenDesktop 3.0 to 7.5,

Veeam backup & cloud connect, VMware Cloud Foundation.

**Languages:** **Intro UNIX, Linux,** C++, COBOL, JAVA, SQL, DOS, HTML

Tools: AWS CloudFront & IAM, IBM ORadar, LogRhythm, Solarwinds, Blue Coat, Netforensics with Cisco, Sourcefire with Cisco, IBM BigFix, Foundstone, Nexpose, Nessus and Comodo, ServiceNow, Cherwell, CA Service Desk, Tipping Point, Check Point, Check Point, Fortinet Firewalls, ASA Firewalls, Symantec, End Point Manager, McAfee ePolicy Orchestrator 3.6.0, Virus Protection Utility, Symantec VIP, MX Logic, Gmail/Google for business, Websense & IronPort Web Filtering & Email Security Appliance, Exchange 5.5, 2000, 2003, 2007 and 2010 Active Directory, MX Logic Utilities, HP Fortify, Encase Forensic 7/8, Entrust Authority Security Manager, Identity Guard Theft Protection and Credit Monitoring, Sailpoint, Oracle Identity Cloud Service, CarbonBlack, IBM BigFix & RESOne.

Education

Bachelors of Science - Information Technology Systems ▪ Trinity University – Washington DC, 2005

Associate’s Certificate - It Project Management ▪ George Washington University, 2005

Associate Degree - General Studies ▪ Prince Georges Community College, 2002