

Alex Baxter

+1(646)948-1130

oarb20@gmail.com

Executive Summary

Security professional of 17 years' experience focusing on managing a broad range of infrastructure, compliance, and cyber security programs to further the development of securing many organizations' infrastructure while guaranteeing regulatory & legal compliance requirements to align with business objectives. Consistently delivering cost effective solutions while actively leading the full lifecycle of project management, engineering, and operations. Managed teams in implementations of advancements to infrastructure & information security programs which align industry compliance standards with the companies' mission in mind. Adept at interfacing with end-users, cross departments, and company executives to identify critical business objectives while effectively translating them into a technical vision strategy, pinpointing & communicating potential risk to minimize any impact.

Core Competencies

- Team building & Professional Development
- Mobile & Cloud Security Technologies
- Infrastructure & Security Solution Architecture Designs
- Vendor Management
- Information Security Governance
- Regulatory Compliance & Data Security
- Business Continuity / Disaster Recovery
- Threat Management & Risk Mitigation
- Security Policy Implementation

Information Technology & Security Industry Experience Diversity

Healthcare & Pharmaceutical

Pfizer • Wyeth • Children's Hospital • Jefferson Health Systems • Temple University Health Systems

Financial Investment & Insurance Services

Prudential • KPMG • Allstate • Moody's Analytics • Allied Mortgage Group • Pacer Financial • 40 North Capital LLC

Legal, Municipalities, Non-Profit & Federal

Akin Gump Law Firm • Environmental Protection Agency • Welfare Rights • Yost & Tretta Law • Phila Gas Works

Retail, Professional Services, Start-Ups

Pepboys • LPQ • HP • mPhasis • Robert Half Technologies • Dexter Technologies • ASI • Jet.com

Accomplishments

Leadership

- Lead and managed the PCI & GDPR compliance for the Information Security Programs to minimize company risk exposure
- Instituted an IT governance body which incorporated key members of legal, IT, HR, operations, & development in order to preside over business technology integration decisions
- Represented company's information security program to senior leadership team and board
- Managed numerous global infrastructure & security teams with the goal of driving the business forward

Strategy & Vision Planning

- Developed a 5-year infrastructure & security roadmap plan to redesign legacy network environments
- Spearheaded a hybrid cloud virtualization architecture with software-defined storage and networking to minimize risk, improve system uptime, and reduce capital expenditure while maximum business productivity.
- Established a mandatory quarterly information security awareness training program targeting all company employees from end-users to executives in order to provide education on major threats, phishing, best practices, and good cyber hygiene.
- Initiated and executed Security frameworks to the business (PCI-DSS, NIST, ITIL)

Team Collaboration

- Facilitated team cohesion and collaboration by heading up the challenge of removing roadblocks to improving workflow, improve business operation, and streamline projects.
- Instituted policies and systems to improve team moral that focused on corporate values that foster work life balance

Project Management

Alex Baxter

+1(646)948-1130

oarb20@gmail.com

- Established & augmented Information Security Services Programs for multiple companies incorporating defensive in-depth castle approach. Leveraging SIEM Security Information & Event Management, Incident Response, Cyber Intelligence Threat Hunting, Risk Mitigation Assessments, Compliance Management, Vulnerability Management, and End-User Security Awareness Training
- Engaged with numerous companies to assess and ensure legal regulatory compliance laws & cyber security framework standards are implemented and met (Sarbanes-Oxley SOX, HIPAA, SOC2, PCI, NIST, ISO270001, FedRamp)
- Directed system integrations projects & teams after acquisition merger of 2 major pharmaceutical companies
- Developed Disaster Recovery & Business Continuity strategic plans leveraging both cloud (AZURE, AWS) and on-premise solutions that reduced current RPOs & RTOs expectancies by 83% with annual and semi-annual test
- Designed numerous scalable physical & virtual datacenters and infrastructure build outs (Active Directory, Exchange, Lync, System Center, Websense, VMware, Network Services & Security Monitoring)
- Implemented IDS & IPS for an Enterprise Network strategically placing firewalls in various locations on the network to present East-West & North-South network traffic for analysis
- Incorporated multi-factor authentication services to the environment to better secure company data and network access
- Implemented & managed an Identity Access & privilege management solution (Thycotic, BeyondTrust, CyberArk)
- Implemented mobile device management platforms (Airwatch & MobileIron)

RECENT EMPLOYMENT EXPERIENCE

LPQ

January 2016 – Present

Head of Infrastructure & Security (US & Europe)

- Developed and led company's PCI & GDPR compliance program.
- Drove the establishment of cross-departmental governance body for the business to provide a clear application of Information Security Policies & Risk Management prior to any project implementations or operational changes
- Managed all IT infrastructure & security vendor relationships to ensuring SLA fulfillment
- Managed a \$10 million global IT budget spend while reducing cost
- Managed a global IT staff and provided professional guidance and development
- Implemented a new endpoint security protection platform (CrowdStrike)
- Architected an enterprise wide defense in-depth information security program and strategy that ensured the integrity, confidentiality and availability for the business
- Orchestrated the organization's disaster recovery and business continuity plans
- Defined processes for data encryption, desktop/server baselining, and user provisioning as it relates to security procedures
- Conducted semi-annual infrastructure, information security gap assessments and audits which included a review of physical, technical and policy controls to safeguard of company data
- Lead efforts to achieve regular successful Level One PCI merchant annual RoC (Report on Compliance)
- Negotiated contract agreements with vendors and contractors
- Integrated multi-factor authentication, SIEM and privilege management solutions to the environment in order to improve data security and access control auditing (Duo, Thycotic)
- Created a security awareness training program for the advocacy of information security company-wide
- Migrated the company to multi-cloud and SaaS platforms (Azure, AWS, O365) for redundant hosting of all critical applications
- Created the IT framework on classification of data
- Established the company's first change control management processes and CAB (change advisory board) to prevent unauthorized business impacting system changes
- Developed scripts for the automation
- Implemented a mobile device management solution to protect the company's data on mobile

Insight Global (Consultant – Moody's, KPMG, Prudential, Allstate)

January 2015 – December 2015

Infrastructure & Security Architect / Associate Director

Alex Baxter

+1(646)948-1130

oarb20@gmail.com

- Managed a team of infrastructure security engineers
- Fostered relationships with other key business and technology leadership stakeholders to implement and influence policy, develop roadmaps and strategy execution, and manage digital risk for the company
- Performed risk assessments against organization's on-premise & cloud infrastructure (AWS, Azure)
- Directed project teams on the review and testing of disaster recovery & business continuity procedures
- Worked with Security Governance teams to update and further develop the user recertification process to include changes implemented as a result of completing an RBAC implementation project.
- Mentored and supervised junior engineering staff for delivery of corporate IT strategy solutions and goals
- Worked with the Identity & Access management Security teams on implementation of new auditing system
- Assisted in the design and migration of the new active/active datacenter
- Instantiated policies based on risk assessments and company business requirements
- Managed and forecasted multiple budgets to eliminate waste overspend
- Wrote custom scripts for automation & reporting on systems for auditing, performance, and system changes
- Managed and monitored SIEM systems for events and directed junior engineers on incident response and remediation
- Worked with all stakeholders to ensure company regulatory compliance
- Assisted in managing all information security projects and initiatives
- Assisted in performing security vulnerability audits and delivered reports to senior leadership team

ASI

July 2014 – December 2014

Manager, Security Consulting/ Senior Systems Engineer

- Lead team to manage multiple clients' vulnerability management programs
- Created documentation for client's infrastructure and security architecture and incident procedures
- Assisted in creation of security incident mitigation and response strategies for client companies
- Managed day to day of clients' endpoint detection and SIEM

PAST EMPLOYMENT SUMMARY

Dexter Technologies (Consultant)

March 2012 – July 2014

Team Lead, Infrastructure & Security

Pfizer (Consultant)

October 2011 – August 2012

Team Lead, Enterprise Systems & Security Architect

mPower

July 2010 – May 2011

Security Consultant

Children's Hospital

Sept 2009 – Feb 2010

Lead Security Consultant

Pepboys

Nov 2007- Feb 2009

IT Specialist

Allied Mortgage Group,

Feb 2007 - Nov 2007

IT Specialist

Robert Half Technology

June 2006 – Feb 2008

Network Security Consultant

Penn State University

Jan 2006 – May 2006

Consultant

St. Joseph's Preparatory School,

Sept 2001 – Dec 2005

(Consultant)

Technology

Windows Server ▪ Meraki ▪ AlienVault ▪ ArcSight ▪ Splunk ▪ OpenVAS ▪ OSSEC ▪ Nessus ▪ Palo Alto ▪ Cisco IOS ▪ Brocade ▪ Mac OS ▪ SonicWALL ▪ Sophos ▪ Symantec ▪ Backup Exec ▪ McAfee ▪ Kaseya ▪ AWS ▪ Azure ▪ Terminal Services ▪ Hyper-V ▪ Barracuda ▪ Exchange ▪ Active Directory ▪ Fortinet ▪ TMG ▪ Palo Alto ▪ Proofpoint ▪ DUO ▪ WSUS ▪ System Center ▪ Citrix ▪ Kali Linux ▪ Websense ▪ OpenDNS ▪ Infoblox ▪ FireEye ▪ IDS ▪ Nmap ▪ VPN ▪ Radius ▪ VMWare ▪ Tripwire ▪ Acronis ▪ EPIC ▪ Wireshark ▪ Commvault ▪ Qualys ▪ Metasploit ▪ AirWatch ▪ MobileIron ▪ ADMT ▪ Office365 ▪ SIEM ▪ Change Auditor ▪ ADFS ▪ Cloud Security ▪ Carbon Black ▪ CrowdStrike ▪ Veeam ▪ PowerShell ▪ Python ▪ Java ▪ MySQL