**MICHAEL SCHANK,** Senior Information Technology Security Manager

Mr. Schank has over 20 years of experience in managing teams and budgets in IT Security, Software Development, Network Administration, hardware and software installation, network support and training. He possesses a broad range of experience in design, development, and implementation of full-stack IT solutions that meet budgets and time constraints. He promotes a team environment that encourages information sharing, accountability of individual team members, and focus on timely delivery of quality solutions.

**WORK EXPERIENCE**

**IT Security Manager, Conduent (formerly Xerox) (2016 to Present)**

**•** Currently manages the six-member team of Senior Security Engineers, Application Security Engineer, and Network Security Engineers that support the *Conduent hosted Network Data Center for the State of Maryland DHR Network consisting of two IBM zSeries Mainframes and hundreds of Linux a*nd Windows servers and a variety of Private and Public facing COTS, Traditional, and web applications. Wrote the Agile Security SOP for Conduent Local and State solutions contract with the State of Maryland Office of Technology and Human Services (OTHS). As Security Manager, he manages the team responsible for the security for all Applications and Application Servers for OTHS. He also oversees the on-site teams responsible for the servers and Disaster Recovery sites for the Maryland Health Benefits Exchange (Obamacare) and the datacenter where Conduent provides infrastructure (security and servers) for other state and local government contracts.

**Senior IT Security Engineer, Xerox (2015 to 2016)**

• Instituted new Web Application Security Program for several Xerox teams of developers. After developing/customizing a crosswalk of FISMA/NIST, IRS 1075, CJI, State of Maryland, and Privacy Controls related to our State of Maryland work, led the development of a web application security policy and 200 item checklist offering security policy guidance to the Xerox Development teams.

• Customized Nessus audit scripts for DOD STIGs and IRS SCSEMs to automatically verify compliance of hardware and software for the Xerox development and production platforms. I oversee and review scheduled and Ad-hoc Nessus Vulnerability and Compliance scanning of over 300 State of Maryland servers hosted by Xerox. Led the 7-member team that reviews the Daily SEIM logs and reports for these servers.

• Worked with State of Maryland OTHS to institute insertion of Security Policies and Process to convert from Waterfall security model to Agile for all Xerox application Development with the State of Maryland Department of Human Resources, inserting a security team member in each critical planning and implementation phase of the Agile process.

• Xerox senior security members who must approve all changes and modifications to operating systems, network devices, databases, and applications for the State of Maryland OTHS servers and applications in our Change Management meetings attended weekly by our team of engineers, developers, and managers.

• Implemented Web Application Penetration Testing program for all new Xerox/State of Maryland Applications using Kali, Nessus, CenzicTrustwave, and OWASP ZAP pentest tools. Developed custom methods for penetration testing.

**Jupiter Systems**- (1996- 2015) JUPITER Corporation spinoff - Technology Services company based in Gaithersburg, MD

**IT Director**- Hired, trained, and managed several Network Administrators and Helpdesk staff to fulfill support contracts. Got Cisco training and certifications in both Sales and Engineering roles to support Small to Medium sized business phone systems and security appliances. Managed the sale and support of many Cisco products. Got Microsoft Cloud BPOS training and achieved SMB Cloud Champion status. Installed and Maintained Office 365 (Exchange, SharePoint and Lync for several insurance companies including Group Dental Service (GDS), Coventry, and Group Vision Service. Transitioned a 100+ staff government-contractor dTS (Development and Training Services) from Exchange On-premise to the cloud, with zero down-time. Moved their local 2010 SharePoint site-collections to the 2013 servers on Office 365. Installed private virtual servers on Azure to federate with Office365 for single-sign-on using cloud Identity Management on Azure AD in hybrid environment. Installed, configured, and maintained VMware Virtual Desktop Infrastructure (VDI) for remote access and high-availability of corporate resources. Setup solutions for encryption on the cloud and PKI Key management through Microsoft EMS/IRM on SharePoint. Use of this and two-factor authentication on Office 365 has allowed FedRAMP compliance with government-mandated security controls on sensitive information stored in the cloud. Transitioned clients from the On-Premise Deltek/CostPoint system to the Cloud-based Deltek systems that leverage Citrix client software. Upgraded PKI Certificates on Web and FTP servers, and upgraded services to use SSL/TLI and SFTP exclusively. Verified all servers were patched for heartbleed, shellshock, and many other vulnerabilities. Monitors security websites daily for the latest news in security. Very strong in Cisco ADSM, CLI, CCM, CUE and other Configuration tools.

2007- **Information Assurance Officer/Network Administrator**- managed the IT services contract to setup and complete Certification and Accreditation (C&A) of the TSA Transportation Threat Assessment center (TTAC). Leased office space, provided all equipment and software, including physical controls, access systems, Surveillance systems, needed to get ATO for the TTAC in Reston for over 100 credentials investigators. Connected our network securely to FBI, State Department, and local law enforcement databases. Held Top Secret/SCI clearance. Setup System Security Plan conforming to NIST-800 and FISMA standards maintained POA&M list. Used Cisco ASA with Syslog and SNORT as IDS system, used Microsoft SCCM and NAC and AD for Access Control, Windows-based Nessus and Linux-based Backtrack Penetration tools, Wireshark, and many other tools to verify and maintain compliance. Built a web-based Case Management database system using MySQL and Ruby on Rails to track all cases from entry, through all stages of approval, and it was used by over 90 credentials investigators for hours every day to document, store, and approve/reject all the work done on every case and subsequent appeals. Used Backtrack to do proxy and SQL vulnerability web software penetration testing on the Linux-based web app. Maintained the network through monitoring controls, patch management, configuration lockdowns and application whitelisting through Group-Policy. Implemented documentation of baselines and strict change management policies and testing procedures to ensure stability and quick remediation of risks found.

2001- **Director Network Administration**- Hired and managed nearly 15 different Network administrators to provide outsource IT services to companies such as: Georgetown Publishing (100+ staff), Padco-AECOM (150+ staff), JUPITER Corporation (100+ staff), Brazilian Naval Commission (100+ staff), SKANSKA, Land Trust Alliance, Posse Foundation, and part-time services to about 50 other businesses in the metro area. Personally installed networks in three cities in Africa for USAID. Supported installs and maintenance of Accounting departments using Deltek/GCS/CostPoint, QuickBooks, Peachtree/Great Plains systems. Installed and maintained web servers and firewalls taking millions of hits per day at peak.

1999- **Software Development Manager**- Hired and Managed team of 3 programmers to sell solutions including: subscription and membership sales database for American Congress on Surveying and Mapping, and sales/inventory databases for two Cartier stores using Visual Basic/Access and SQL. Both stored sensitive accounting and customer data, including credit card numbers.

1996- **IT Sales Manager**- Managed sales department of new tech spinoff company. Sold many contracts in software development and Network service and Support contracts. Setup company project-based accounting system using QuickBooks. Novell consulting led to providing Oracle and Web-Sphere assistance under contract with the Brazilian Naval Commission in Washington (CNBW). This led to setting up cascading Linux firewalls and DMZ configurations to protect sensitive data. Updated the firewalls regularly for several years to maintain security. Eventually moved Oracle from Novell to Linux servers.

**JUPITER Corporation**- (1992-1996) government-contractor firm based in Wheaton, MD

1995- **Director IT/Physical Resources**- Managed reception and Helpdesk staff. Provided Network Administration and began sales of IT solutions: hardware integration and software development. Installed and maintained Deltek accounting software.

1994- **LAN Administrator**- server and helpdesk support to 40-node HQ Novell network. Telecommunication support

1992- **Technical Writer/Editor**- Supported various headquarters projects as well as support to DOE, Office of Defense Programs (DP) as editor and writer for their 1993 Five-Year Plan

**EDUCATION**

**University Nevada Las Vegas**. 1983-1985 Engineering School- FORTRAN, COBOL, Work compiled on Harris Mainframe- After nearly two years spent abroad in France, Transferred to Maryland

**University of Maryland, B.A., 1989**, French Language and Literature, minor in Mechanical/Materials Engineering

**CERTIFICATIONS**

ISC2 CISSP Certification

Cisco SMB Select Engineer Certification

Microsoft Certified Professional

Novell Certified NetWare Engineer (CNE)

Microsoft OEM Authorized System Builder

CompTIA A+ Certified Computer Technician certification

Novell Authorized Partner

Lexis-Nexis Certified Independent Consultant (for law practice support)

**Clearance Held- DHS Top Secret/SCI Clearance 2010**

**Technical Proficiencies-**

**SECURITY:** Cisco ASA Firewalls, SonicWALL Firewalls, LogRhythm SIEM/SIM/SEM, CISCO Hardware IPS, Snort/Suricata NIDS, SSL certificate configuration and management, Symantec Cloud Endpoint Protection AntiVirus/HIDS, Splunk

**NETWORKING**: WinCap/Wireshark/NetworkMiner packet analysis, DNS servers, DNS records management/zone files/transfers, DNS Blackhole, DHCP Servers/IP address management, WiFi Access Points, SMTP mail servers, Cisco Routers, Netscan, Apache/Tomcat hardening, IIS hardening, Exchange Hardening

**Vulnerability/PENETRATION TESTING:** PWCrack, Aircrack, OPhcrack, SQLmap, nmap, netdiscover, Cisco Audit tool, Nessus/Tenable, OpenVAS, Burpsuite, MetaSploit, DBProtect, AppDetective

**PATCH MANAGEMENT/NETWORK ACCESS CONTROL:** Microsoft SCCM, Microsoft Intune, Group Policy Application Whitelisting, Regression testing sandboxes, KACE/Dell System Deployment, Symantec SEP/NAC

**OPERATING SYSTEMS:** Windows XP,7, 8, 10; Windows Server 2003, 2008, 2012, 2016; Linux including RedHat, Novell/CentOS, Ubuntu, Xbuntu, Debian, BackTrack, and Kali- Hardening expertise in all desktop, Server, and applications listed.

**DATABASE:** MS SQL, MySQL, MS Access, SQL Queries, Oracle on Novell and Linux, LightSwitch

**Web Development:** PHP, Ruby on Rails, WordPress, Drupal, SharePoint, DreamWeaver CS6

**App Development:** Visual Studio 2015, Visual Basic, ODBC/SQL

**Regulatory Compliance:** FedRAMP, NIST, FISMA, IRS 1075, HIPAA, PCI, Privacy Law

**LANGUAGES/SCRIPTING**: Python, Perl, HTML, CSS, Java, Basic, C+, Powershell, Bash Shell

**VIRTUAL/CLOUD:** VMware Horizon 5 VDI infrastructure deployment, Microsoft Azure Storage and VMs, Office 365 Exchange/SharePoint Hybrid Migrations, AWS, GoogleMail/GoogleDocs/Postini, Microsoft Enterprise Mobility Suite for data encryption/revocation (IRM) and Data Loss Prevention across all endpoints including BYOD.

**COUNTRY EXPERIENCE**

I have worked in France, Belgium, and Burundi.

**LANGUAGES**

**English-** US Citizen

**French**- (Certification from Paris Chamber of Commerce and Industry Business French exam- received highest mark- “Excellent” showing proficiency in oral, comprehension, and written French.