Bryce R. Porter
bryceporternc@gmail.com
mobile: 336-601-2858

3069 Cumbie Road
Winston Salem, NC 27107

Career Objective
To affect positive change in the fields of Information Technology and Cyber Security while working to develop new and better ways of leading and managing the teams that provide those capabilities to an organization.

Current Position

July 2018 to Present
Chief Information Security Officer, The University of North Carolina at Greensboro
Greensboro, NC

- Executive leadership responsibility for all Cyber Security, IT Risk, and IT Compliance Management functions at an R2 research university with ~3000 faculty & staff serving 25,000+ students.
- Strategic thought leader responsible for establishing and maintaining the enterprise security vision, strategy, architecture, and multi-year roadmap to ensure that the university's information resources are adequately protected.

Responsibilities include:

- Lead the development of enterprise-wide security policy, standards, processes, and risk profiles influencing both institutional and divisional strategy.
- Develop and implement a strategic, long-term organizational strategy and resourcing roadmap to ensure sufficient resources exist to sustainably protect University information resources.
- Lead and coordinate enterprise-scoped activities supporting strenuous compliance with FERPA, HIPAA, PCI-DSS, ISO/IEC 27002, NIST 800-53, NIST 800-171, and NIST CSF regulations, standards, and requirements.
- Act as the champion for the enterprise information security program and foster a security-aware culture across the University. Lead the development of up-to-date information security policies, procedures, standards, and guidelines, and overseeing their approval, dissemination, and maintenance.
- Establish an IT Risk Management program and working with senior leaders across the university to codify risk tolerance at institutional and divisional levels. Implement a controlled program of risk identification, analysis, and treatment procedures with programmatic methods for mitigating risks to acceptable levels.
- Provide periodic reports and updates to the Executive Committee and the Board of Trustees, and provide subject matter expertise on security standards and best practices to University senior leadership.
- Oversee the evaluation, selection, and implementation of information security solutions that are innovative, cost-effective, and minimally disruptive. Partner with enterprise architects, infrastructure, and applications teams to ensure that technologies are developed and maintained according to security policies and guidelines.
- Develop, mentor, and manage a high performing staff of multi-disciplined information security professionals.
- Fulfill the duties of University Records Officer, leading efforts to ensure compliance with public records laws and the University records retention & disposition schedule.
- Fulfill the duties of DMCA Agent for the University, actively discouraging copyright violations and ensuring that violators are removed from the network with appropriate disciplinary actions.
- Act as IT Disaster Recovery Coordinator, assembling and updating Continuity of Operations and Disaster Resilience & Recovery plans for the IT Services division, and coordinating all recovery and continuity efforts.
- Chair the University's information security advisory committee, Identity & Access Management Governance Committee, GDPR Working Group, the UNC Information Security Council (comprised of CISO's at all 17 UNC institutions).
- Co-chair or participate in an ex-officio capacity on the Data Governance Council, HIPAA Compliance Committee, Risk Management Subcommittee, and Compliance Management Subcommittee.
- Coordinate and maintain adequate levels of cyber liability breach insurance sufficient to protect the university's interests in the event of a security breach. Oversee incident response activities and the investigation of security breaches. Assist with any associated disciplinary, public relations and legal matters. Liaise with law enforcement and other advisory bodies as necessary to ensure that the organization maintains a strong security posture.
- Develop metrics to measure the effectiveness of the security management program and increase the maturity of the program over time.
- Monitor the industry and external environment for emerging threats and advise relevant stakeholders on appropriate courses of action.

Accomplishments thus far include:

- Sought and received funding to increase cyber security staffing resources by 300%. Developed and implemented a scalable organizational model comprised of four distinct functional areas: Security Operations, Security Systems

Engineering, Security Architecture & Assessment, and Risk & Compliance Management. Added several new technology tools to support an expanded scope of activities and functions.
- Created the University's first dedicated Cyber Security Operations team equipped with enterprise-class SEIM (Splunk), threat intelligence (FireEye), vulnerability management (Rapid7), data protection (Varonis & Spirion), cloud security (Azure & GCP), anti-malware (Microsoft ATP), network behavior anomaly detection (Stealthwatch), digital forensics (FTK), and packet capture (Endace) tools.
- Introduced procedures for application development security including static application security testing (SAST), dynamic application security testing (DAST), content/composition analysis, and application-level penetration testing.
- Oversaw and led the effort to introduce tools and processes for monitoring and managing third party risk using BitSight.
- Implemented tools in the ServiceNow platform to administer Governance, Risk, and Compliance programs with automated production of artifacts for audit response.

Prior Experience

March 2017 to July 2018
Enterprise Security Architect, The Clearing House
Winston-Salem, NC
- Enterprise-level responsibility for the security components of core payments systems at a Systemically Important Financial Markets Utility (SIFMU) providing over $2 trillion USD in payment services per day.
- Portfolio-level governance of the design, implementation, and sustainment of all Information Security systems, solutions, policy, processes, standards, and procedures.
- Responsible for constructing and delivering executive-level briefings on the security design of core payments systems to CISO-level leadership at 25 of the country's largest banks and the Federal Reserve Board.
- Provided information security leadership, design direction, and consulting services for the construction and implementation of the nation's first Faster Payments system (TCH Real Time Payments) using the first ever real-time payment messaging and settlement technologies in the US.
- Provided information security consulting and advice required to achieve PCI-DSS and PCI-TSP compliance certification for the first ever private credit card PAN data tokenization platform (TCH Secure Token Exchange) to be used by large US banks in partnership with card networks (Visa & MasterCard) and digital wallet providers (Samsung & Apple) for secure credit card payments on mobile devices.
- Initiated construction of an Enterprise Architecture program, including adoption of a top-level Enterprise Architecture approach (TOGAF) as well as Enterprise IT Architecture, Information Security Architecture, Software Architecture, and technology-specific Component Architecture documentation governing the design and integration of technology systems across the enterprise.
- Designed and implemented significant improvements for a comprehensive software security development and testing program using HP Fortify & WebInspect tools for Static and Dynamic Application Security Testing (SAST & DAST) and Black Duck for software composition and Open Source content analysis.
- Initiated migration of software development from legacy SDLC "waterfall" style to more Agile style practices, including integration of DevOps and DevSecOps toolchains involving industry-leading tools such as UrbanCode, Jenkins, Maven, Gradle, Jira, JFrog Artifactory, ALM (Quality Center)
- Initiated adoption of Docker containers and software orchestration using Kubernetes for select projects
- Provided leadership and execution support for enterprise-wide penetration testing program, including requirements definition, vendor selection, scope, method, target selection, and remediation activities.
- Constructed budget proposals for program-level sustainment activities as well as one-time improvement projects for select Information Security technologies.
- Provided direct input and support to senior executive leadership for organizational changes, hiring decisions, job descriptions, professional development programs, and industry involvement activities.
- Provided input to regulatory activities involving FFIEC, FISMA, PCI-DSS, PCI-TSP, NIST, DISA, CIS, ISO, GLBA, and GDRP regulations and requirements.

July 2014 to February 2017
Children's Ministry Director, Creative Director, The Summit Church
Kernersville, NC
- Provided vision, direction, and leadership for large volunteer-driven organization providing weekly services to 2000 families in three locations across the Piedmont Triad area of North Carolina.
- Led multi-site organization consisting of 8 paid staff and interns supporting 150+ volunteers
- Recruit, train, and empower staff and volunteers to provide music, programming, technical and non-technical service elements via consistent leadership, coaching, and training initiatives.

- Designed, planned, coordinated, and executed custom multi-day summertime camp events involving 700+ kids and 400+ volunteers.
- Managed and administered ministry finances and budgets, performance management cycles, improvement initiatives, and ministry goals.

March 2014 to July 2014
Director of Information Security, The Clearing House
Winston-Salem, NC

- Responsible for day-to-day support of information security systems, processes, and personnel for a Systemically Important Financial Markets Utility (SIFMU) providing over $2 trillion USD in payment services per day.
- Led and supported a team of seven information security professionals with responsibility for all internal and external information systems securing electronic payments for 25 of the largest US financial institutions.
- Focused areas of responsibility include threat & vulnerability management, intrusion detection/prevention, incident response, digital forensics, penetration testing, malware prevention, software security, network security architecture, systems acquisition & integration, encryption & PKI services, policy & process management, risk management, and team member hiring & development.
- Responsible for construction and maintenance of an end-to-end secure software development lifecycle process, executing static and dynamic code analysis, 3rd party code review, and regular security testing to identify and remove vulnerabilities and weaknesses in custom-developed software during development and testing cycles.

September 2011 to March 2014
Network Technology Manager, Wells Fargo Bank
Winston-Salem, NC

- Manager of the Network Engineering, Logical Network Services (LNS) team. LNS is accountable for implementing and supporting critical foundational network infrastructure systems providing DNS, DHCP, IP Address Management, NTP, and Internet Web Proxy services across the entire Wells Fargo enterprise.
- Individual responsibilities include leadership, management, coaching, and support for a team consisting of 33 engineering and operations team members (24 FTE, 5 contractors, 4 offshore), within the Technology and Operations Group (TOG), Technology Infrastructure Services (TIS), Enterprise Technology and Production Services (EPTS), Network Engineering Services (NES) line of business.
- Line-level leadership and management of three separate working teams with distinct technology responsibilities and processes:
    - LNS-Proxy – accountable for maintaining and supporting enterprise Internet web proxy systems supporting nearly 100% of the company's outbound Internet traffic.
    - LNS-DNS DDI Engineering – accountable for maintaining the enterprise DDI (DNS/DHCP/IP Address Management) infrastructure, and developing monitoring and automation tools.
    - LNS-DNS DDI Operations – accountable for managing and manipulating DNS, DHCP, and IP Address Management records for the enterprise. Also accountable for managing the company's Internet domain presence, including brand protection services
- Built a high-performing team of experts through proactive resourcing and hiring, restructuring of the team, clear role definition, granular goal-oriented performance management, and skill/competency development of individual team members.
- Led a comprehensive process improvement program to significantly improve operational and engineering processes. Results included significantly reduced production problems and error rates while simultaneously increasing volume of output.
- Led efforts to assemble a complex 3-year project business case and successfully pursued funding for the purchase and implementation of the next-generation DDI system for the enterprise, posturing the infrastructure to meet long-term requirements for capacity, functionality, scalability, security, and emerging technologies (IPv6, DNSSEC, others).
- Manage strategic vendor relationships with Infoblox, BlueCoat, MarkMonitor, and Milestone Systems (integrator).
- Manage budget and financial forecasting activities for $3MM baseline resources budget. Assist with budgeting and forecasting duties for several components of a $400MM (approx.) annual network infrastructure equipment and maintenance budget.
- Developed and maintained critical internal technology partnerships with upstream and downstream partners including the Internet Services Group, Data Center Management, End User Computing, Computing Platform Services, Application Delivery Controllers (Load Balancing), Information Security Technologies, Enterprise Architecture, Infrastructure Architecture, and others.
- Developed and maintained strategic LOB technology relationships with Wealth Brokerage & Retirement, Wholesale Banking, Mortgage & Lending, Retail Banking, Insurance Services, and others.
- Achieved and maintained compliance with strenuous availability goals for network infrastructure systems.

- Greatly improved the health and auditability of routine configuration management processes resulting in improved audit scores and reduced operational risk.
- Responsible for leading and managing the timely delivery and execution of complex technology initiatives for network infrastructure systems.
- Implemented a program of process maturity assessments and improvements in order to identify gaps leading to potential improvements.
- Manage costs and pursued saves in support of cost reduction and efficiency goals.

January 2009 to August 2011
Information Security Technology Manager, Wells Fargo Bank
Winston-Salem, NC

- Lead a team of 22 engineering and program management team members (13 FTEs, 9 contractors) in the Information Security Technologies, Network Security group within the Technology and Operations Group (TOG), Technology Governance Services (TGS) line of business, accountable for implementing and supporting critical network security infrastructure systems.
- Manage three working teams with disparate technology processes:
    - Network Security Advanced Engineering – accountable for testing and certifying new and improving network security technologies in preparation for production deployment, and for providing 3rd level escalation support for production problems on network security infrastructure systems.
    - Network Security Management Systems – accountable for supporting and maintaining enterprise-wide firewall management systems, IDS/IPS systems, network access control systems, Wireless LAN security systems, and monitoring and automation tools for the enterprise network security infrastructure.
    - Network Security Program Management – accountable for supporting the Network Security merger integration program (co-managed with a Program Manager).
- Lead and manage the timely delivery and execution of complex technology initiatives for firewalls, IDS/IPS, AAA, and WLAN systems.
- Increase sustainability of network security systems through the implementation of an active program to comprehensively test and certify new and improving technologies for network security systems.
- Achieve and maintain compliance with strenuous availability goals for network security technology systems.
- Deliver on key merger integration initiatives, including both organizational and technology integration goals.
- Manage strategic vendor relationships with Cisco, Check Point, IBM ISS, Tipping Point, Breaking Point, Log Logic, Motorola, McAfee, and Accuvant (VAR).
- Execute budget and financial forecasting activities for $1.6MM baseline personnel resources budget. Assist with budgeting and forecasting duties for $12MM (approx.) annual equipment and maintenance budget.
- Conduct strategic and tactical planning efforts to ensure the continued growth and improvement of technology systems and teams.
- Manage all phases of the technology lifecycle for critical network security systems.
- Analyze and assess workflow performance and technical process performance in order to identify gaps leading to potential improvements.
- Manage costs and pursue saves in support of revenue goals.
- Develop and maintain service offerings for testing and certification services, technology management services, and production monitoring and support services.

November 2007 to December, 2008
Network Security Manager, Wachovia Bank
Winston-Salem, NC

- Manage and lead a team of 8 FTEs and 3 contractors in the Corporate Information Security (CIS) group within the Operations, Technology, and E-Commerce (OTE) business unit accountable for implementing and supporting critical centralized network security infrastructure management systems.
- Develop and improve repeatable business and technology processes in support of Network Security technology objectives and initiatives.
- Maintain and support centralized network security management systems for firewalls, IDS/IPS, AAA, and WLAN systems.
- Implement a program of Continuous Process Improvement aimed at achieving objectives in the Capability Maturity Model Integration (CMMI) and IT As A Business (ITAAB) initiatives.
- Develop and implement efficient, repeatable, and measurable human processes for employing network security technologies and centralized management systems for distributed network security infrastructure systems.
- Develop relationships and maintain strategic working partnerships with other internal technology groups, including Network Services, Network Architecture, Network Engineering, Network Operations, Security Operations, Data Transmissions, and Availability Management.
- Coordinate and provide internal and external audit responses for network security systems and teams.

- Manage and maintain strategic vendor relationships with Cisco, Check Point, IBM ISS, Crossbeam, Nokia, Secure Passage, and Forsythe Solutions (VAR).
- Coach and mentor mid- to senior-level network security engineers and contractors in the performance of technical responsibilities and functional competence areas.
- System Owner and System Manager (SM) for 6 critical network security technology systems.
- Develop and implement the local organization's approach to Application Portfolio Management (APM), leading to increased stability and supportability for several key network security infrastructure systems.
- Provide oversight for technical change management.
- Implement a 24x7 monitoring and alerting system aimed at increasing the capabilities for managing the availability, capacity, and performance of network security systems.
- Translate strategic technology goals and objectives from senior and mid-level management into tactical performance goals for engineering team members.
- Implement metrics-based approach to measuring and improving system and team member performance.

May 2006 to November 2007
Senior Network Security Engineer, Wachovia Bank
Winston-Salem, NC

- Design and implement highly-available application-layer transparent proxy firewall solution using Secure Computing (now McAfee) Sidewinder firewalls in production data processing environments.
- Lead engineering project team on multiple merger integration efforts, including Golden West/World Savings and A.G. Edwards.
- Lead and mentor engineering team in the deployment, support, and ongoing maintenance of Check Point firewalls.
- Design, document, automate, and socialize a seamless upgrade path for firewall technologies designed to minimize downtime and business impact during deployments.
- Coordinate with business units and stakeholders to create comprehensive implementation, testing, verification, and backout plans.
- Construct comprehensive process documentation to ensure project continuity.
- Perform engineering-level project management duties, including task management, resource allocation, budgeting, and scheduling.

October 2004 to April 2006
Information Security Subject Matter Expert, National Center for the Study of Counter-Terrorism and Cyber-Crime at Norwich University (NOTE: Name has since changed to Norwich University Applied Research Institutes)
Northfield, VT

- Provide subject matter expertise in the areas of Information Security, Information Warfare, and Information Operations to 229th Information Operations Squadron, Vermont Air National Guard, as directed by the Air Combat Command, US Air Force
- Install, maintain, and operate multi-site network attacker/defender laboratory/simulation environment based on standard Air Force network systems.
- Author and deliver online Advanced Distributed Learning (ADL) courses for Network Defense (NetD), Network Warfare Operations (NW Ops), and Network Operations (NetOps) for the US Air Force.
- Develop experiential learning techniques for hands-on ADL-delivered training, simulations, and military exercises.
- Facilitate course delivery and provide supplemental instruction in the areas of NetD, NetOps, and NW Ops.
- Implement and enhance Learning Management Systems using customized open-source software tools.
- Provide subject matter expertise for Continuity of Operations planning and development.
- Provide ancillary mission support for simulation range and learning management systems.

March 2003 to September 2004
Senior Information Security Engineer, VeriSign, Inc.
Dulles, VA

- Provide information security services for critical DNS infrastructure of the Internet, including for A and J Root servers, SRS system, and global constellation of gTLD DNS servers serving the .COM, .NET, and .ORG domains.
- Provide information security services for National Critical Information Technology Infrastructure systems, including the .COM and .NET domain registries and VeriSign PKI root certificate systems, as well as the SS7 cellular backbone signaling system and other critical revenue-generating systems.
- Architect, deploy, manage, and maintain load-balanced Check Point firewalls and Juniper/NetScreen VPN systems in Cisco routed and switched network environments supporting multiple production, corporate, and QA/development service environments.
- Provide PKI Administration services, including management and back-end technical support for Managed-PKI service line.

- Conduct incident response, forensic investigation, vulnerability assessment, penetration testing, risk assessment, and internal IT self-audits.
- Provide comprehensive network security engineering services for purpose-built production environments, including Site Finder, RoamerView, J-Root Anycast, Managed DNS, and others.
- Provide application security services for internally-developed applications during development, QA, deployment, and sustainment portions of the application life cycle.
- Install, manage, and maintain highly-available firewall, VPN, and IDS systems for globally disparate corporate and production processing environments.
- Provide network engineering, system administration, application development, scripting, process management, and peer group management services.

March 2001 to March 2003
Senior Information Security Engineer, Network Solutions, Inc.
Herndon, VA

- Deployed, managed, maintained, and administered firewalls, intrusion detection systems, authentication systems, and host-based security for industry-leading domain name registrar production environment
- Security engineering design and implementation of a multi-tiered, highly available security architecture for entirely new production data center, resulting in zero lost-revenue security or operational incidents from implementation to present.
- Designed, implemented, and managed distributed intrusion detection system for production environment, providing intrusion data to support numerous successful internal and external investigations.
- Provided 24x7 support for production security systems, including incident response, performance tuning, troubleshooting, and problem resolution.
- Instituted strong encryption, authentication, and access control systems for management of production environment in efforts to eliminate all cleartext logins.
- Functioned as primary administrator of Public Key Infrastructure for certificate-based authentication of VPN systems.
- Lead engineer for network security architecture, design, and integration projects, including $12 million data center migration, HA firewall implementation, VPN integration, and numerous mergers/acquisitions.
- Developed and instituted policies and procedures for security incident response team, including development of Chain of Custody documentation and Security incident lifecycle processes.
- Provided application security engineering and review services for internally-developed web-based applications during development, QA, deployment, and sustainment portions of the application life cycle.
- Designed, implemented, and managed multi-tiered logging system to support network and security device infrastructure, which became vital to day-to-day network and security support, management, and troubleshooting efforts.
- Designed, installed, and managed a production out-of-band console access solution for production servers, network equipment, and security equipment that utilized encryption and strong authentication controls.
- Developed and implemented custom host-based security measures, including lockdown/hardening scripts, routine assessment scripts, and access-denial alert scripts.
- Developed and implemented periodic external and internal penetration testing exercises, including test plan development, tool development, vulnerability analysis guidelines, and reporting procedures.
- Performed forensic investigations of numerous systems, including an exploited public FTP server, several rooted Linux systems, and a instance internal data theft by a contractor.
- Performed several security awareness briefings, including IDS brown bag lunch, Incident Response Team training, and a VPN vendor-interoperability technical briefing.
- Performed routine investigation and research of publicly-announced security vulnerabilities, viruses, trojans, and other security-related announcements.
- Assisted System Administrators with development of standard secure OS configurations for Solaris, Linux, AIX, and Windows systems.

March 2000 to February 2001
Senior Network Security Engineer, Para-Protect, Inc.
Centreville, VA

- Lead and managed security engineering teams on customer engagements, performing comprehensive networking and security consulting services for Fortune-500 customers.
- Provided network and security architecture design, engineering, implementation, assessment, testing, and managed security services for customers.
- Performed security assessments of customer network infrastructures, including firewalls, routers, switches, IDS, VPN, and physical security systems.

- Lead engineering team accountable for the design and implementation of a revenue-generating managed security services and network monitoring system for customer network security infrastructure systems.
- Conducted internal and external penetration testing, web application testing, OS security testing, and social engineering tests during customer engagements.
- Performed router, switch, firewall, VPN, and IDS product evaluation, research, and testing in highly-interoperable, vendor-agnostic testing lab.
- Performed pre-sales engineering and customer relationship development, including trade show interactions, executive briefings, and engineering assistance.
- Performed project management duties for extended-length customer engagements, including customer relationship management, billable time accounting, coordination of engineering efforts between teams, task and resouce management, and management of project documentation.
- Developed custom cross-training program for engineers and project/account managers, including cross-disciplinary skill development and peer review processes.
- Delivered security assessment and engineering reports and presentations to customer executives and operational personnel.
- Coordinated follow-on engineering and assistance efforts for customers, including technical assistance, engineering assistance, and on-demand call support.
- Performed research and development of security tools, vulnerabilities, and exploits, including participating in building an industry-leading security vulnerability database for use in custom report generation.

November 1996 to March 2000
Sr. Network Engineer/Network Security Manager, Raytheon
Kwajalein, Marshall Islands

- Performed enterprise-wide management of a 1200+ node WAN employing multiple WAN, LAN, and security technologies, including Frame Relay, T1, ISDN, dial-up, and VPN connectivity to multiple international sites.
- Functioned as lead engineer on several infrastructure improvement projects, including campus-area network installation for local school system, metropolitan-area network installation for local retail stores, and backbone performance improvements that increased LAN speeds from 10Mbps to 100Mbps.
- Functional role of Network Security Manager operating under DoD-appointed Network Security Officer.
- Functioned as lead engineer for ground-based communications for command, control, and communications for solar-orbiting satellite systems.
- Performed implementation and management of a secure ISP-style Internet access system supporting a community of over 3000 people.
- Installed, maintained, and managed firewalls, routers, switches, and bandwidth allocation devices in multiple diverse military and commercial environments.
- Performed design, installation, management, and support duties for multiple secure network operating systems including Novell NetWare, Windows NT, Sun Solaris, and DEC Unix.
- Responsible for LAN equipment configuration, installation, management, monitoring, and security.
- Performed design, installation, management, and support duties for multiple departmental and enterprise-wide email systems, including upgrades and platform migrations.
- Performed continual network security risk assessment duties, including periodic review of external and internal networks and monitoring of vulnerability and exploit announcements.
- Performed documentation, accreditation, and training duties as required by AR-380 and AR-25IA.

August 1995 to November 1996
Senior Field Engineer, Raytheon
Portsmouth, RI

- Performed design, configuration, installation, and project management of small and medium scale enterprise networks (up to 1000 nodes) for customers, including servers, clients, application software, cabling systems, network equipment, security equipment, and wide area communications.
- Designed and installed a secure multi-point ISDN WAN for a municipal secure data communications project, connecting municipal offices with police and fire departments.
- Project management, design, and installation of several medium-scale networks at public and private schools, including the infrastructure and server systems for North Providence High School (RI) and a fiber-optic campus-area network at Avon Old Farms private school in Avon, CT.
- Performed project management duties for installation teams, sub-contractors, and support personnel.
- Developed and delivered custom training programs for system administrators.
- Performed pre-sales engineering and sales support for network consulting business.
- Performed network and security engineering duties for consulting customers.

March 1995 to August 1995

Network Systems Engineer, DXM Computers, Inc.
East Providence, RI

- Performed comprehensive network systems design and consulting duties for the installation of customer networks.
- Provided logistical planning, consultation, and coordination services for installation of network systems for customers.
- Performed LAN & WAN installations, including cabling, network equipment, servers, workstations, and application software.
- Provided network security design, implementation, and management services, including custom policy creation and implementation of automated enforcement measures.
- Performed several hundred network server platform installations for customers.
- Provided customized training services for support personnel.
- Evaluated new products and emerging technologies for business development group. Provided engineering-level support to business executives regarding new products and opportunities.
- Developed, managed, and executed government sales and municipal contract bidding processes for fledgling government sales business, including RFQ/RFP completion and representation at bid openings/signings.
- Provided engineering assistance and strategic planning in conjunction with retail sales team

February 1993 to March 1995
Senior Network Technician, Image Solutions, Inc.
North Providence, RI

- Performed design and installation duties for small network infrastructure customers, including servers, workstations, cabling infrastructure, and network equipment.
- Performed installation and support of secure networks for small to medium size customers, including lending institutions, real estate offices, retail stores, and manufacturing firms.
- Provided pre- and post-sales support for network installation customers, including functional role as primary customer contact for technical issues.
- Performed customer network infrastructure design and architecture review duties.
- Designated lead hardware technician for custom Intel-based server design, assembly, and installation.
- Performed pre-sales technical support for customer engagements.
- Conducted technical employee training and mentoring.
- Created and implemented multi-tiered escalation process for PC/network support team.

Education & Certification

- Bachelor of Science in Management Information Systems (BS, MIS) from Liberty University
- Graduate Certificate in Cyber Security from The Bryan School of Business and Economics at UNC Greensboro
- Certified Information Systems Security Professional (CISSP) (2004)
- Check Point Certified Security Expert (CCSE)
- Certified DoD Information Systems Security Officer (ISSO)
- Certified Novell Administrator (CNA)
- RSA Certified Systems Engineer
- ISS Certified Product Specialist for RealSecure, System Scanner, and Internet Scanner
- Graduate, Air Combat Command Classroom Instructor Course
- Graduate, Air Combat Command Instructional Systems Design Course
- Hubbell Premise Wiring Certified Installer for CAT 5 Cabling Systems
- Previously held licenses in Rhode Island and Massachusetts as a Telecommunications Systems Contractor
- Formerly held DoD Secret Security Clearance (DISCO, 2003)
- Secondary education including classes at University of Maine, Community College of Rhode Island, Norwich University, and Liberty University

Technical Competencies

- **INFORMATION SECURITY:** Expert knowledge of network security systems, including extensive experience with a wide variety of products from leading network security technology vendors, including Check Point, Cisco, Juniper/NetScreen, IBM ISS, Tipping Point, Ixia, Secure Computing/McAfee, RSA, and Cylink (frame encryptors only); Expert knowledge of IPSEC VPNs; Expert-level knowledge of AAA/authentication systems and protocols, including TACACS, RADIUS, EAP (all forms), and 802.1x; Extensive experience with VeriSign Public Key Infrastructure (PKI) and various encryption and digital signature software; Extensive experience with common security assessment and testing tools, including Foundstone, Qualys, Nessus, Nmap, Strobe, PingSweep, John the Ripper, L0phtCrack, etc.; Extensive experience with IDS/IPS systems from IBM ISS (Proventia and

RealSecure), Tipping Point, Entrerasys (Dragon), and SourceFire (Snort); Working knowledge of NBAD technologies, primarily Lancope StealthWatch.

- **NETWORKING:** Expert-level knowledge of TCP/IP (v4 and v6) and multi-protocol internetworking, including comprehensive understanding of network communications through all layers of the OSI model; Moderate to extensive experience with a wide range of network products from Cisco, Juniper, Nortel (Bay Networks, Synoptics, Wellfleet), Nokia, HP, Xyplex, Lucent (Ascend), Shiva, DEC, Digital Link, 3COM; Foundry, Alteon, and F5; Working knowledge of common dynamic routing protocols (BGP, OSPF, RIP, RIP2, IGRP, EIGRP) and switching technologies (Spanning Tree, MPLS). Working understanding of VoIP, Multicast, and QoS technologies.
- **WIRELESS COMMUNICATIONS:** Extensive experience with wireless LAN (a/k/a Wi-Fi) products and protocols, including 802.11a/b/g/n standards, 802.1x authentication, and wired/wireless network integrations; Significant experience with cellular wireless technologies including GSM, CDMA, and SS7 backbone signalling.
- **OPERATING SYSTEMS:** Extensive experience with Linux, Solaris, AIX, Windows (3.0 and upwards); Moderate experience with FreeBSD, OpenBSD, HP-UX Unix systems; Past experience includes in-depth working knowledge of deprecated network operating systems, including Artisoft LANtastic, Microsoft LAN Manager, and Novell NetWare; Extensive experience with IBM, Sun, Dell, HP/Compaq, and ALR server hardware platforms; Significant experience with complex server architectures, including SMP and MPP systems, RAID arrays, Beowulf clustering, ESX virtual servers, and SAN systems.
- **SYSTEMS MANAGEMENT:** Extensive experience with SNMP-based network management technologies, including Tivoli Enterprise, HP OpenView, BindView EMS, InfoVista, Nagios, MRTG (including Cricket and the RRD Tool), Citrix MetaFrame, and Veritas software products; Moderate experience with vendor-specific product management tools including CiscoWorks, Nokia Horizon Manager, and NetScreen Global Pro; Extensive experience with several different helpdesk, asset management, and call tracking software applications, including Heat, Remedy, Infra, and What's Up Gold.
- **SOFTWARE DEVELOPMENT:** Moderate experience with Java, .NET (C# & VB), Visual Basic, SQL, PERL, JavaScript, and COBOL; Introductory experience with DevOps tools including Jenkins, UrbanCode, Ant, Maven, Gradle, Jira, JFrog Artifactory, ALM (Quality Center), Docker, Kubernetes; Extensive experience with DevSecOps tools including HP Fortify, WebInspect, Black Duck

Professional Organization Memberships/Affiliations

- Information Systems Security Association (ISSA)
- Computer Security Institute (CSI)
- Association for Computing Machinery (ACM) Special Interest Group on Security, Audit and Control (SIGSAC)
- International Information Systems Security Certification Consortium, Inc. (ISC)²