**John Madison Benson III**

**15249 Coachman Terrace**

**Woodbridge, VA 22191**

**Cell: 845-641-5800**

[**John.M.Benson3@gmail.com**](mailto:John.M.Benson3@gmail.com)

[**www.linkedin.com/in/johnmbenson3**](file:///C:\Documents%20and%20Settings\bensonj\Desktop\www.linkedin.com\in\johnmbenson3)

**Summary**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

An Information Technology Professional with 30 years of experience. Primary expertise in: Information Security, Information Privacy and IT Audit, in verticals which include the Technology, Consumer, Government, Healthcare, Financial, Telecommunications, Manufacturing, Industrial and Consulting Markets.

**CLEARANCE**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

TOP SECRET

**CertificationS**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RSA Archer Certified Administrator

FSCA - ForeScout Certified Administrator

CISSP - Certified Information Systems Security Professional

CEH - Certified Ethical Hacker

EnCE - Encase Certified Examiner

TCNU - Tenable Certified Nessus User

CHFI - Computer Hacking Forensics Investigator

ECSA - EC-Council Certified Security Analyst

LPT - Licensed Penetration Tester

CIPP/G - Certified Information Privacy Professional / Government  
CHA - Certified HIPAA Administrator

CNDA - Certified Network Defense Architect

NSA 4011 - National Security Agency Information Assurance Certification  
CBCP - Certified Business Continuity Professional

CIW-SA - Certified Internet Webmaster-Security Analyst

CIW-DDS - Certified Internet Webmaster-Database Design Specialist  
CIW-WDS - Certified Internet Webmaster-Web Design Specialist  
CCSE - CheckPoint Certified Security Expert  
CSS - Cisco Security Specialist  
SCE - Sniffer Certified Expert  
CCNP - Cisco Certified Network Professional  
CCDP - Cisco Certified Design Professional  
MCSE - Microsoft Certified Systems Engineer  
CNA - Certified Novell Administrator  
NETWORK+ - CompTIA Network+ Certification  
PROJECT+ - CompTIA Project+ Certification

**Professional experiencE**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Senior Cyber Security Analyst / RSA Archer Technical Lead**

Makpar Corporation

November 2015 – Present

* Supporting the Internal Revenue Service (IRS), Office of Cybersecurity division in the deployment of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) risk management program
* Supporting as-is analysis and solution architecture activities related to CDM and continuous monitoring
* Leading IRS tool strategy and gap analysis initiatives to assess existing tools and capabilities across the enterprise with the goal of reducing redundancy and cost
* Providing technical support to the IRS for the RSA Archer Migration from CSIRC to Eops, that includes a new build of the hardware and software in a clustered virtual environment and an upgrade from RSA Archer version 5.5 to 6.1
* Working with IRS Tool Owners to create RESTful API Web Services to integrate tool source data into RSA Archer for reporting
* Configuring custom RSA Archer Front-End Solutions and Application, while also performing the Operation & Maintenance duties on the Back-End

**-2-**

**Senior Security Engineer / CDM Team Lead**

Knowledge Analytics

March 2015 – August 2015

* As the CDM (Continuous Diagnostics and Mitigation) Team Lead for the Federal Aviation Administration I lead a team of Engineers in the Phase 1 design of the CDM Architecture
* Wrote 2 white papers detailing the specific tasks associated with Consolidated Inventory and Dashboard Design
* Lead and participated in the drafting of the ISCM (Information Security Continuous Monitoring) CONOPS for the FAA in compliance with the NIST SP 800-137
* Built an RSA Archer Dashboard Prototype that incorporated the imported FAA data from CSAM, BelManage, BigFix and Forescout

**Director of Technology**

Missing Link Security / PHYLEO

July 2013 – December 2014

* As a key member of the Quick Response Team (QRT), conduct independent assessments of clients’ infrastructure and security controls. Perform federal security test and evaluation efforts related to FISMA, DHS 4300A, and/or NIST 800-53 including Vulnerability Scanning/Analysis, Penetration Testing and Remediation
* Perform as the company’s Computer Forensics Investigator, using Encase v7. Conducts examinations of all digital media, develops Investigative Plans to perform the investigation and analysis, responsible for recovering deleted, hidden and encrypted data. Thorough understanding of hardware and data recovery, evidence handling, chain of custody, evidence storage, use of sterile media, forensic imaging techniques, cracking system and file passwords, detecting steganography with signature analysis
* As the Director of Technology for both Missing Link Security and PHYLEO, oversee all technical issues including IT Design, Engineering and Support as well as supporting Business Development in both the proposal process and in the delivery process

**Cyber Security Technical Lead**

Missing Link Security

October 2011 – July 2013

* As the Technical Lead for the Cyber Security Division at Department of Commerce, US Patent and Trademark Office (USPTO), applied and managed a large and complex portfolio of continuous monitoring processes for the federal client. Facilitated Risk Assessments, Security Test and Evaluation (ST&E), Contingency Plan Testing, and remediated POA&Ms
* Performed as the company’s Computer Forensics Investigator, using Encase v7. Conducted examinations of all digital media, developed Investigative Plan to perform the investigation and analysis, was responsible for recovering deleted, hidden and encrypted data. Had thorough understanding of hardware and data recovery, evidence handling, chain of custody, evidence storage, use of sterile media, forensic imaging techniques, cracking system and file passwords, detecting steganography with signature analysis
* As a Contractor Side Lead for Archer Deployment Project at Cyber Security Division (USPTO), primary duties include implementation of the RSA Archer Risk Based Management Tool as per USPTO requirements, act as primary interface to RSA Archer Development Team and provide them sample data for testing & development, supervise overall progress to ensure all the project deliverables are completed on time and meet the customer requirements
* Provided leadership and mentoring to a team of 35 Cyber Security Analysts

**Information Assurance Subject Matter Expert**

SRA International

January 2010 – September 2011

* As an Information Assurance Subject Matter Expert at the Department of Treasury, Bureau of Engraving and Printing was responsible for leading a group of nine Cyber Security Analysts ranging from Junior to Senior. Responsibilities included reviewing/revising project developed FIPS 199 categorizations, system security plans, security impact assessments and privacy impact assessments. Additionally, was responsible for developing and reviewing system hardening guides. Performed as a technical resource/mentor for the project team.
* Performed Security Risk Assessments, Gap Analysis, Documentation, and Vulnerability Assessments. Produced written reviews and recommendations and delivered in the form of an Audit Report.

**-3-**

**Senior Technical Business Analyst**

EKI Consulting

March 2009 – June 2009

* As a member of an 8-person team, performed as the Senior Technical Business Analyst for the Walmart Pharmacy/Vision HIPAA Security Remediation Program. Tasked with the supervision of 2 Technical Business Analysts, designed and implemented solutions to the failure to detect alterations and deletions of ePHI data at rest, lack of encryption of ePHI data in transit and unauthorized/undetected access to systems

**Senior IT Auditor/Information Security Consultant**

Jefferson Wells

March 2005 – March 2009

* Senior IT Auditor with SOX and HIPAA compliance experience with clients such as Dun & Bradstreet, TIAA-CREF, MVC Capital, MARCOR, Biolab, Minntech BV, AIG, Jackson Hewitt, Seedco, United Bank for Africa, Coinmach and Wyndham Worldwide. Projects ranged from assessing IT controls according to GAGAS and ISACA frameworks to assisting the client with documentation of policies and procedures; narratives and process flows for 4 main areas: a) security; b) software development life cycle; c) change and problem management; and d) backup and recovery. Additionally, assisted in security administration remediation of gaps and weaknesses
* Performed Data Security Audits, Security Risk Assessments, Gap Analysis, Documentation, Penetration Tests and Vulnerability Assessments. Produced written reviews and recommendations and delivered in the form of an Audit Report
* Performed Business Process Improvement and PII Data Privacy Audit for SEEDCO. The objective of this engagement was to review the procedures and controls over the current operation, to identify opportunities for improvement and deficiencies, and prepare implementable recommendations

**Independent Consultant**

Bensico Network Solutions

February 2003 – February 2005

*Multiple Consulting Projects*

**HIPAA Security Project Manager**

UMass Memorial Medical Center

November 2004 – February 2005

* Performed Project Management tasks to ensure compliance with the Final HIPAA Security Rule

**Security Architect**

Department of Veterans Affairs

June 2004 – November 2004 & February 2005 – March 2005

* Performed Audits, Security Design, Gap Analysis, Documentation, Penetration Tests and Vulnerability Assessments. Audits included the use of Reconnaissance and Footprinting, Vulnerability Scanners, Sniffers, Spoofing Tools, Brute Force and other Password Cracking tools. Provided HIPAA Compliance, Networking and Security consultation

**Senior Information Security Analyst**

Department of Treasury, Internal Revenue Service

November 2003 – March 2004

* Performed Audits, Security Design, Gap Analysis, Documentation, Penetration Tests and Vulnerability Assessments. Audits included the use of Reconnaissance and Footprinting, Vulnerability Scanners, Sniffers, Spoofing Tools, Brute Force and other Password Cracking tools
* Evaluated the organization’s security and risk management program to determine the security of a networks design and evaluatedDisaster Recovery Plans

**Senior Information Security Analyst**

Department of Commerce, Bureau of Economic Analysis

September 2003 – November 2003

* Performed Audits, Security Design, Gap Analysis, Documentation, Penetration Tests and Vulnerability Assessments. Audits included the use of Reconnaissance and Footprinting, Vulnerability Scanners, Sniffers, Spoofing Tools, Brute Force and other Password Cracking tools
* Conducted FISMA Certification & Accreditation evaluation for the Information Assurance section of the network infrastructure
* Determined whether the computer systems and network infrastructure are in compliance with the NIACAP, NIST or industry best practice security policies and standards
* Conducted training sessions on topics such as Networking and Security Awareness

**-4-**

**Senior Information Security Analyst**

Inspector General of Federal Housing Finance Board

August 2003 – October 2003

* Performed Audits, Security Design, Gap Analysis, Documentation, Penetration Tests and Vulnerability Assessments. Audits included the use of Reconnaissance and Footprinting, Vulnerability Scanners, Sniffers, Spoofing Tools, Brute Force and other Password Cracking tools

• Conducted FISMA Certification & Accreditation evaluation for the Information Assurance section of the   
 network infrastructure

• Determined whether the computer systems and network infrastructure are in compliance with the NIACAP,   
 NIST or industry best practice security policies and standards

• Conducted training sessions on topics such as Networking and Security Awareness

**Senior Security Specialist**

Verizon

March 2002 – January 2003

* Provided support for Verizon Enterprise Solutions salesforce of 50+ Corporate Account Managers and 60+ Sales Engineers regarding Security and Internet related topics. Regional coverage area encompasses the entire State of New Jersey covering all verticals. Accomplished task of selling 3.1 Million Dollars’ worth of security solutions and products
* Provided HIPAA and CIPA consultation
* Performed Verizon standardized evaluations to include Penetration Testing, Risk Analysis, Policy Review, VPN and IPS/IDS
* Conducted In-House training seminars for Sales Engineers and Executive Security Briefings for CIO/CTO level Clients

**Senior Network Engineer**

New York Presbyterian Hospital

March 2001 – December 2001

***Hired as consultant to perform the following:***

* Network comprised of Cisco Equipment to include: 70 Routers, 170 Switches and 10 ATM Switches with a variety of Hubs. Network is a fully redundant EIGRP and IP/IPX environment with multiple Campuses and Remote Sites
* Assigned supervisory role of Lead Engineer supported by 5 Engineers and a 24/7 Help Desk. Primary duties were comprised of managing infrastructure projects between the Cornell and Columbia Medical School networks to include providing LAN/WAN support
* Completed the design, configuration, and implementation of a Remote Access VPN solution
* Project managed a network-wide IOS upgrade on all routers and switches to conform with contractual SLA and documentation of the LAN/WAN infrastructure
* Configured, Installed and Monitored the Cisco IDS sensors and responded to security breaches
* Converted the once Public Class B network to a more secure network using Checkpoint/Nokia Firewalls and NAT

**Internetwork Solutions Engineer**

Thrupoint Inc

January 2000 – January 2001

*Multiple Consulting Projects*:

**Morgan Stanley**

* Configured and implemented 100MB Fast Ethernet and Full Duplex links, HSRP redundancy and IGRP routing protocol with RIP redistribution
* Handling configuration and deployment of the Market Data Branch Sites Firewall Infrastructure and implementing LAN upgrades
* Upgrade of the Cisco PIX Firewall. Configured and implemented EDMZ and IDMZ Cisco routers and switches. Also upgraded the LAN infrastructure to include moving all ethernet segments from WAN router and shared hubs onto dual Cisco 5509’s with RSM’s

**Cisco Systems**

* Worked as part of an 11-member team of Internetworking Solution Engineers (TAC) to develop a troubleshooting tool (Output Interpreter). Tool can be found on the Cisco Web Site under CCO. Tool was developed through use of Cisco’s proprietary scripting language (Maven), and enables troubleshooting for a wide range of networking problems based on analyzing show command output. Created the first analysis ever of a “Show Running Configuration” command

**-5-**

**Network Design Engineer**

AT&T Solutions

November 1998 – January 2000

*Hired as consultant to perform the following:*

* Responsible for providing Network Designs and Integration Documentation for Client locations Worldwide. Wan Designs comprised a variety of technologies including OSPF, Frame Relay, Dedicated T1, T3 and ISDN, Created Out Of Band Management via terminal servers over POTS lines. Implemented High Speed Encryption with Cylink Encryptors.
* Provided full detailed packages to include: Cabling Diagrams, Cisco Router Configurations, Misc. equipment, cable order lists, and step by step site installation procedures
* Most recent designs included Citicorp’s Backbone Infrastructure for North America and the integration of several Core Hub and Feeder sites for domestic Internetwork

**Internetwork Consultant**

KPMG

January 1998 – November 1998

* Responsible for a wide range of consulting assignments dealing with LAN/WAN solutions, including evaluation, LAN/WAN design, router configuration and implementation
* Provided 3rd level support for remote access issues regarding the SecurID network. Included were Ascend and Cisco routers, Ascend ISDN Pipeline, Shiva Lanrovers and Radius server
* Configured, Implemented and Project Managed token ring to ethernet conversion followed by a 4,000 workstation Windows NT rollout while working on the Woolworth project
* Completed survey of cabling and PBX installations at various schools as part of the Contract with the NYC Board of Education.
* Conducted a walk thru inspection of several NYC Dept. of Finance facilities and Evaluated the needs and requirements for future installation of imaging system

**Senior Telecommunications Analyst**

PRODIGY Internet

August 1997 – December 1997

*Hired as consultant to perform the following:*

* Responsibilities included troubleshooting connectivity issues related to the 500+ node LAN/WAN and evaluating capacity problems
* Using tools such as NV/6000, PROCOM and U.S. Robotics Total Control Manager. Monitored and configured routers and modem chassis at remote sites

**Network Engineer**

IBM Global Services

September 1995 – July 1997

*Hired as consultant to perform the following:*

* Responsibilities included monitoring and troubleshooting 1,000+ nodes LAN/WANs for Campbell Soup Company and Rhone Poulenc, Inc.
* Using network tools such as NetView/6000 for AIX and Intel Landesk I remotely managed the networks consisting of Cisco, Cabletron, Novell, and Windows NT
* Handled such duties as configuring Cisco routers, assigning TCP/IP addresses, assisting users and logging trouble tickets using DP Umbrella

**Network Administrator**

WilTel Data Network Services

January 1995 – August 1995

*Hired as consultant to perform the following:*

* Monitored a 476 node WAN consisting of Cisco, Welfleet routers and Synoptics hubs via SNMP on a UNIX SunSparc Station
* Created new user accounts and login scripts on a Novell network. Created trouble tickets using Paradigm

**Senior Computer Operator**

Liquid Air

October 1993 – June 1994

*Hired as consultant to perform the following:*

* Managed console of IBM 3090 including running batch jobs and starting CICS sessions
* Duties also included training new operators to run the console and various peripherals

**-6-**

**Systems Engineer**

Bank of America

August 1990 – April 1993

* Monitored performance of IMS, CICS and network in an IBM ES/9000 MVS/JES3 environment
* Performed DB loads and backups using CA-7

**Senior Network Operator**

Federal Reserve Bank of New York

November 1987 – June 1990

* As a senior member of the Banks first Disaster Recovery Site I performed Contingency Tests in accordance with the Disaster Recovery Plan
* Managed system and network activity to ensure integrity and availability
* Performed IPL’s, complete power up/down, stand-alone dumps, spool offloads and IML’s

**Senior Computer Operator**

Panasonic

March 1986 – October 1987

* Monitored CICS and ran batch jobs on an IBM 3081 JES/2 mainframe
* Duties also included training new operators in the tape library and print room

**Air Defense Artillery**

United States Army

March 1984-July 1985

* As a Short Range Missile Crewman I was the Driver of a Chapparel Missile Launcher.
* Discharged under Honorable Conditions

**Education**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bachelor of Science, Information Security, Western Governors University (expected completion 06/17)

07/94-01/95, 03/87-10/87, 10/85-03/86: Computer Learning Center - Paramus, NJ

Computer Networking: Novell Netware, AS/400, MS-DOS, MS-Office, MS-Windows, and Word Perfect

Computer Programming: Cobol, Assembler and RPG II

Computer Operations: OS/JCL and DOS/VS1

11/12-12/12: Guidance Software

EnCase v7 Computer Forensics I

EnCase v7 Computer Forensics II

EnCase v7 EnCE Prep Course

04/15-06/15 EMC

RSA Archer Admin

RSA Archer Admin Advanced

**TECHNICAL AFFILIATIONS**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ISACA - Information Systems Audit and Control Association

ISC2 - International Information Systems Security Certifications Consortium

IETF - Internet Engineering Task Force

ISSA - Information Systems Security Association

IAPP - International Association of Privacy Professionals