

Don G. Kuecker, CISSP, QDSP
P.O Box 12836
Tallahassee, Florida 32317
850-201-0073 - Office
480-236-0158 – Cell
850-668-6963 – Home
DGKPHX00@yahoo.com
Don@dgk-eseurity.com
www.DGK-eseurity.com

EXPERIENCE:

AmbironTrustWave
Security Consultant

Jan 2007 – Present

Utilize my many years of experience and combine the need for enforcing PCI DSS (Payment Card Industry – Data Security Standards) to the various players (Issuers, Acquirers, Payment Gateways, Service Providers, Merchants and others) in conjunction with AmbironTrustWave developed procedures and services that address the security needs of the credit card community. Provide adhoc consulting services for the various clients in assisting them with compliance issues and requirements. Develop and advise on new security measures or findings that contribute to the overall security requirements of the financial industry and other industries as a whole. Streamline compliance validation processes to include tools and procedures that can be reused and provide additional control over for the subjective nature of the same.

NetSPI – Genworth Financial
VoIP Security Specialist

Nov 2006 – Dec 2006

Provide guidance in developing and processing a VoIP Security Assessment as part of a multipoint assessment process for Genworth Financial. Test security readiness of client's VoIP solution as they are preparing their global presence for its usage to ensure they are in compliant with various regulations and privacy concerns now and as they go forward. Provide best system/security recommendations that include authentication and integrity of their VoIP data packets that match their vendor chosen VoIP product based on previous successes and new endeavors going forward.

FCSO (First Coast Service Operations, Inc) - Blue Cross & Blue Shield Florida
HIPAA Compliance Consultant **Sept 2006 – Nov 2006**

Guide client through the processes of establishing job definitions for their claims processing department (CMS – Center for Medicare & Medicaid Service) as a preparatory step in defining basic job roles that will be the foundation for implementing a centralized identity management tool to be decided. Guide client through the systematic development of planning, testing and implementing RBAC (Role Based Access Controls) to ensure compliance with authorization processes that addresses HIPAA-SA (Health Insurance Portability & Accountability Act – Administrative Simplification) and other regulatory requirements.

Walt Disney World
Security Advisor

Dec 2005 – Sept 2006

Assist with the interpretation, definition and implementation of security checklists that ensure/enforce PCI (Payment Card Industry) Data Security Standards for any new and existing applications that require credit card data or information across the corporation enterprise. Assist with efforts to establish an enterprise logging effort that specifically addresses PCI DSS requirements that provide adequate audit logs and will address SOX (Sarbanes Oxley) needs also. Lead efforts that entail initial security involvement with new or altered applications/solutions at their introduction into the enterprise in conjunction with the various business entities and new initiatives. Assist with the various security requirements in regards to wireless type endeavors that include WPA (WiFi Protected Access), Symbol APs(Access Points) utilizing Afaia and AppCenter as a centralized control solution for inventory and security management that incorporates KERBEROS as a network authentication protocol. POS (Point of Sale) Symbol devices running Windows Mobile 2003 (PPC 2003) and various other solutions required to facilitate the needs of a world class organization. Lead efforts to develop a Minimum Security Baseline for wireless type devices that include various PPC (Pocket PC – Windows Mobile 2003), Windows Embedded XP, Kerberos authentication, and various current wireless technologies. Assist with initiative to establish security controls for a SOA (Services Oriented Architecture) based on the Microsoft .NET and VAP (Vignette Access Portal) infrastructure that can address various security aspects of SOX, PCI and similar regulatory requirements for an extensive web based environment. Lead a new initiative to incorporate an application security design architecture for the development community of this client. Provide adhoc security expertise where needed within the security team, provide interpretation of security assessment reporting and findings, fill unknown security requirement needs as they arise.

Levi Strauss & Company
SOX Security Remediation Consultant

Sept 2005 – Nov 2005

Provide assistance with various SOX (Sarbanes Oxley) material security weakness findings specifically with 1.) Segregation of Duties. 2). Identity Management. 3.) Third party connection access control and monitoring. 4.) Security policy & procedures development. Assist development team with planning, testing and implementation of IBM Tivoli Identity Manager in regards to moving all User ID and Password management off individual platforms onto a more centralized solution and thereby addressing various security issues, establishing a base for an identity management life-cycle and providing the means to reconcile account identities and their associated user attributes (access privileges/entitlements). Assist with various security related items – Syslog/audit trail disposition, Security Awareness training, and others.

Siemens Information & Communications Networks, Inc Sept 2004 – Sept 2005
Principal Security Engineer

Provide security team direction and support assisting Siemens obtaining a DISA/FSO Information Assurance Certification for their VoIP (Voice over Internet Protocol) implementation that will allow them to market this offering to the various DoD (Department of Defense) agencies such as the USAF and others. This includes such things as testing the design solution utilizing GR81502, GSCR-Appendix-3, VoIP STIG (Security Technical Implementation Guide), Gold Disk process, Network STIGs, Operating system STIGs (UNIX, Windows (Windows 2003 Server – Domain Controller-Active Directory & Windows XP Professional), SQL Server 2000 Database & others), C2VGLAN specifications, and various Best Security Practices ensuring the security readiness compliance. Build various security mitigation controls such as firewall solutions, security policies, operating system security hardening efforts (UnixWare, Cisco IOS, Windows 2003 Server-DC-AD, Windows XP Professional, SQL Server 2000 database, Web servers – Apache), VPN solutions, Access Control setups, Administration role definitions and others. Interfacing with the various auditing entities/IA (Information Assurance) such as JITC (Joint Interoperability Test Command), DISA (Defense Information Systems Agency), numerous vendors such as Foundry Networks, Beyertone, NICE, DAKS, and others on behalf of Siemens. Providing Project Management in regards to defining detail tasks, defining time lines, projecting required skill sets for onsite engineer staff requirements. Provide hands-on skills for network infrastructure configuration which includes such things as VLAN setup, VLAN tagging (QoS) setup, PIX firewall setup, various ACL (Access Control Lists) for separating and protecting VoIP traffic versus non-VoIP traffic accordingly, IPSec VPN configuration/implementation, network security hardening (Foundry Networks). Provide accountability role in regards to interfacing with the various auditing/testing administered by BAH (Booze Allen Hamilton) compliance experts addressing all security related issues.

**Florida DOH (Department of Health)
Security Consultant**

Jul 2004 – Aug 2004

Assist DOH (Department of Health) SIT (Strategic Information & Technology) Division in identifying gaps within their Security Architecture, Interpreting STO (State (of Florida) Technology Office) newly mandated security rules that now incorporate various NIST SP800 publications, NIST FIPS specifications, Carnegie Mellon Software Engineering Best Security Practices, ISO 17799 (Common Criteria) guidelines and the HIPAA – Title II – Administrative Simplification – sections 164.308, 164.310 & 164.312 for inclusion into their agency level policies, procedures, guidelines & standards. Review agencies existing technology implementation to identify security related gaps, define a process to include application level security review to meet various regulatory agency requirements and retroactively validate the security readiness of the various application services provided by the DOH both to Internet and Intranet type user communities. Working with the DOH security team, provide security guidance with items such as SSO (Single Sign On) solution, network infrastructure controls, security roles required to address various gaps within the entire application life cycle process and others.

**SeNet International Corporation
Principal Security Engineer**

Mar 2004 – June 2004

Assist with C&A (Certification & Accreditation) definition process for DOI (Department of Interior) in accordance with associated guideline. Define/expand usage of SP 800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems) in supporting C&A (Certification & Accreditation) efforts for BIA (Bureau of Indian Affairs) applications and support systems. Lead certification effort for BIA VoIP (Voice over Internet Protocol) by defining specific ST&E (System Testing & Evaluation) items as a future guide for other agencies within DOI. Lead security assessment efforts for DOL (Department of Labor) - OSHA, new web application being developed for Internet use, perform security tests with industry accepted tools such as Nessus, Nikto, OAT, Netcat, Nmap, HTTP sniffer, Achilles, Tigertools and others, analyze results, prepare report with findings, provide recommendations for remediation and assist client accordingly. Assist with Corporate plans to expand business opportunities, define business goals, promote business awareness with federal and commercial customers.

FVAP (Federal Voting Assistance Program)
Lead Security Engineer for SERVE
(Secure Electronic Registration and Voting Experiment)

Nov 2003 – Mar 2004

- Provide team leadership for assessment team. Advise FVAP (Federal Voting Assistance Program) Project leader and other FVAP members in areas of security design, availability requirements, physical security, personnel security requirements, auditing controls, and other requirements. Interpret required agency regulations into meaningful testing and auditing steps as part of the certification process. Advise and assist prime vendors (Accenture, Avanade, Verisign, Hart and others) in regards to security requirements based on Federal, State regulations and Best Security Practices from such sources as NSA, NIST, SANS, DISA, Common Criteria and others. Assess security readiness of infrastructure based on defined test criteria using such tools as ISS, Harris Stat Scanner, NMAP, Nikto, Nessus, Superscan, MBSA, and others. Provide technical interpretation and recommendation for various options as project took directional changes. Prepare final C&A (Certification and Accreditation) output for application.

DoD

May 2003 – Nov 2003

DITSCAP Security Certification Specialist

- Interpret DITSCAP (DoD Information Technology Security Certification and Accreditation Process) requirements in regards to various DoD security mandates (DISA – Defense Information Systems Agency), define/develop SSAA(System Security Authorization Agreement) with designated the ISSO (Information Systems Security Officers), at the direction of the DAA (Designated Approving Authority), perform the appropriate SRR (Security Readiness Review)/testing using the corresponding STIG (Security Technical Information Guides) and accompanying security checklists (Phase III testing of SSAA), applying best industry security practices utilizing tools such as Harris Stat Scanner, Nessus, Nmap, GFI LanGuard, RAT, dig, Libwisker, Nikto, report findings and provide appropriate mitigating controls if needed. My prime responsibility was to certify (C&A) the security readiness of the network infrastructure that includes – firewalls (PIX), routers (Cisco), IDS, DNS (MetalP), Remote access, Hubs/switches, wireless devices(Air Fortress), Mail relay/SMTP, network management components, DMZ and others. Provided C&A (Certification and Accreditation) efforts, testing results and remediation recommendations for major online ordering system. Assist with C&A process for Common Systems – Windows 2000 workstations and HP-UNIX application server platforms.
- This effort requires adequate security clearance – currently working with interim security clearance until full security clearance granted.

Don Kuecker & Associates
Security Specialist

Oct 2002 – Apr 2003

- Design, implement and support DSL/IP utilizing low end Cisco 678 series router/ modem for SOHO.
- Design, implement and support wireless (802.11b) AP (Access Point) for SOHO requirements utilizing WEP, and other security techniques for this technology.
- Assist with Check Fraud forensics efforts for the National Check Fraud Center and local authorities – on going.
- Assist with security testing of new firewall appliance – netMind for local market.
- Provide tutoring efforts for CISSP and CCNA candidates during various stages.
- Design, implement and support IDS – SNORT (network based IDS) for SOHO.
- Design, implement and support secure FTP server, PGP in conjunction with secure e-mail.
- Security assessment for various independent business owners in local area providing recommendations for anti-virus protection, firewall needs and regulatory interpretations as required.

TRW/United States Air Force
Network Security Engineer

July 2002 – Oct 2002

- Design and development of centralized control for managing data and voice based security solutions as it relates to various products such as firewalls(PIX 525 version 6.0), IDS (Intrusion Detection Systems – Cisco Secure IDS – formerly NetRanger), various Cisco switching devices (Cisco 6509 Catalyst Series Switches) monitoring products (such as HP Openview, CiscoWorks 2000– Cisco Network Management, Resource Manager Essential and others), DNS management utilizing QIP.
- Initial setup, configuration and testing of new software upgrades for SideWinder firewall.
- Verification of all components for SideWinder Firewall.
- Security hardening efforts for SideWinder Firewall.
- Development of test turnover procedures for upgrade of SideWinder firewall product from release 4 to release 5 for the Air Force.
- Planning pre-site visit and installation of ETM TeleWall firewall for multiple Air Force facilities.
- Conducted training of ETM TeleWall product for TRW engineers.
- Provided consultation regarding use of ETM TeleWall for Air Force Base personnel in regards to setting up policies, installing client and server software, defining dial plans, normalizing monitor output from appliances, configuring appliance settings, generating reports, establishing user rights and various other support activities.

- Provide security consultant efforts that specifically address possible security needs for Internet, Intranet and Extranet applications to ensure the business objectives of integrity, confidentiality and availability are met.
- Provided security review and recommendations for a multi-vendor multi-billion dollar out-sourcing/out-tasking requirements. Performed multiple and varied due diligence processes and developed a governance model for this implementation of the same. Assisted with the security parameters for joining internal network infrastructure of American Express with out-sourcing partner (AT&T Solutions and IBM Global Solutions) – this included designing the DMZ (Demilitarized Zone) portal, the firewall ACL (Access Control Lists), TACAS definitions for authorization to Cisco devices on network, establishing access logging servers, utilizing Cisco Network Management CiscoWorks as a configuration change monitor and defining basics for a governance model between the various entities.
- Assisted with development of various Policies, Standards and Procedures as they relate to security issues such as Minimum Security Baseline for all applications, password maintenance, secure file transmission such as SSL, encryptions key management, data classification and many others. Was part of core group that addressed encryption key management by developing an indepth policy that defined how to use various cryptography methods such as one-way hashing (SHA-1) with salt for password storage usage.
- Assisted with PKI efforts in regards to CA (Certificate Authority) – for issuing digital certificates, usage of x.509 standard protocols, CRL (Certificate Revocation List) – for validating digital certificates, digital signatures (for authentication and integrity), certificate lifecycle management, the development of a CPS (Certification Practice Statement) and others.
- Assisted with a complete review of existing security policies and procedures in an attempt to develop new procedures based on a Common Criteria (ISO17799/BS7799) approach.
- Part of core group utilizing and advancing JAVA based security solutions using tools such as JDK 1.1 (signing of applets), Java Crypto wrapper, Java 2 SDK, EJB design and usage, Java applet sandbox design, and others.
- Due diligence in regards to third party hosted solutions and other related requirements.
- Review of new technologies in regards to security implications such as wireless applications (WEP, WAP, I-Mode and others), hardware and software technology security solutions, single sign on solutions, encryption solutions, host based IDS – Tripwire, SSL accelerators and many others.
- Work with all stakeholders of business solutions to ensure the effort will enable the business based on varied solutions and interim steps to ensure the safety of the client brand and customer information is maintained.
- Assist with the base operating system builds regarding security hardening for Windows NT and Windows 2000.
- Assist with review and design of firewall (PIX 5xx) design, ACLs for third party access portals, and IDS (Cisco Secure IDS), Tripwire design and placement.

- Assist with security design of web complex, third party access portals, that included various entities such as routers, data switches, various servers, monitoring tools and others.
- Assist with various assessment processes both internal to client and third party hosted solutions.
- Performed various security assessment efforts for client's global security baseline requirements that included sites in England, Italy, North Carolina, Minnesota, Arizona and partially in Australia.
- Network recon using ISS Internet Scanner, interpretation of results, detailed and executive reporting.
- Modem detection efforts with detail and executive level reports.
- Telephone switch scanning with detail and executive level reports.
- LAN capture analysis with detail reports showing TCP/IP connections (unknown routes being passed).
- Router analysis that showed misconfigured packet filters and router connections.
- Miscellaneous site requests such as X.25 assessment, VTAM exit controls, and others.
- This often required interaction with corporate officer level, tactful working skills, excellent written and oral communications, ability to diffuse volatile situations, advanced technical and problem solving skills.

American Express/SecureLogix Corporation
Senior Voice Security Engineer

July 1999 – Mar 2001

- Assist with development, testing and implementation of new product for telecommunications security industry (ETM-TeleWall and others).
- Assisted with the development of educational courses in the areas of telephony security issues, modem detection and basic telephony information
- Provided lead support for Beta site installation, testing, debugging and implementation of new telecommunications security product offerings.
- Provide Security Consulting services for American Express in the areas of E-commerce security design review, integration of various voice and data applications such as Voice over IP, Wireless data communications, CTI (Computer Telephony Integration) and various Internet/Intranet/Extranet web enabled financial application offerings.
- Provide on site system engineer (pre-sales, install and follow-up – customer care) support for telecommunications security products as needed for various beta customers.
- Assisted with the initial training criteria for the TeleWall product line and various iterations such as design, implementation, integration and reporting. Provided many of the key aspects of telephony for these training courses as they currently appear today.

American Express/ Net Access Inc.
Senior Voice Security Engineer

May 1998 – July 1999

- Lead several voice/data security assessment projects at American Express that spanned thirteen months globally.
- Utilized various data assessment tools (ISS and others) to gather information, review, analyze, correlate relevant security vulnerabilities into a two phase reporting process (one for operations staff, one for executive briefing).
- Developed Voice Security Assessment process working with subcontractor services.
- Developed Router configuration assessment process.
- Developed a process to combine voice and data security assessment process as a customer deliverable.
- Develop installation procedures for PIX firewalls strategy.
- Developed Modem/FAX detection methodology.
- Designed, installed and maintained Intrusion Detection systems (Cisco NetRanger – now Cisco Secure IDS) for American Express financial services group.

Mayo Medical Centers
Telecommunications Engineer

1994 - 1998

- Design, implement and support major voice , voice mail, and data communications systems based on Lucent (now Avaya) telephone switching technologies (System85, G2 & G3).
- Design, implement and support Call Center Applications for primarily inbound calling.
- Design, implement and support CTI (Computer Telephony Integration) application utilizing an electronic appointment feature with telephony features.
- Design, implement and support Call Accounting System and Call Management Systems.
- Design, implement and support an ATM (Asynchronous Transfer Mode) solution to replace existing legacy transmission mode for voice, video and data.
- Design, test, implement message exchange protocol to port Voice Mail information to Microsoft Exchange server via POP3 utilizing Lucent product offering.

Mayo Medical Centers
Senior Systems Programmer – Data Networks

1988 - 1994

- Design, implement and support initial WAN/LAN (Wide Area Network/ Local Area Network) routed (TCP/IP) and bridged data network.
- Design and convert Cisco IGRP (Interior Gateway Routing Protocol) proprietary to OSPF (Open Shortest Path First) standard routing protocol.
- Design, implement and support large TCP/IP (Transmission Control Protocol/Internet Protocol) network spanning several states.
- Design, implement and support FDDI (Fiber Distribution Data Interface) backbone for data transmission.
- Design, implement and support DECNET systems for LU62 interface.
- Design, install, and upgrade various Cisco router technologies for LAN/WAN described above.

Saint Mary's Hospital
Senior Systems Programmer – MVS

1986 - 1988

- Design, implement and support MVS/JES2 operating systems.
- Lead DOS to MVS conversion project.

Abbott Northwestern Hospital
Manager Technical Services Group

1983 - 1986

1985 - 1986

- Manage/lead group of technicians in support of all major operating systems, communications systems, maintenance requirements, planning, designing and installing required hardware/software for Information Services department.
- Provide 5-year plan for Information Services department that included anticipated mergers, 50 % growth in technology usage, business continuation planning, processor upgrades, budgetary planning for maintenance – full time employees – hardware – operating systems – LAN/WAN growth and others.
- Provide technology leadership for application departments in their quest for technology usage that would provide competitive edges in health care.

Senior MVS Systems Programmer

1983 - 1985

- Design, implement and support MVS/JES2 operating systems.
- Lead DOS to MVS conversion effort.
- Design, implement and support initial fiber based LAN for hospital campus.

Sperry Corporation
Principal Systems Programmer

1981 - 1983

- Design, implement and support MVS/JES3 operating systems.
- Design, implement and support NCP systems.
- Provide technical assistance with government bid to replace existing Air Traffic Controller hardware and systems.

Jostens
Systems Programmer

1976 - 1981

- Design, implement and support MVS/JES2 operating systems.
- Assist with all program conversions from DOS to MVS.
- Design, implement and support introduction of CICS and online applications for corporate usage.
- Assisted with the initial design, implementation and support of IDMS relational database system.
- Provided system support and development efforts for first online applications for corporate usage (macro level and system level).

Additional work history provided upon request.

Certifications:

QDSP PCI DSS (Payment Card Industry Data Security Standards) audit certification. CISSP Certified Information Systems Security Professional, DITSCAP Mandatory Security CBT, DITSCAP certification, NetRanger Intrusion Detection System CCNA Cisco Certified Networking Associate Cisco Router Software Configuration SMP/E System Modification Program/Extended MVS System Programmer DEC VMS System Management VAX DECNET Management UNIX Internetworking UNIX Security for Systems Administrators TCP/IP Implementation CMS Call Management System Intuity Audix Administration T1/T3 Installation and Troubleshooting ETM Enterprise Telephony Management – TeleWall Integration DCS Definity Communications System (G2 & G3) CICS Customer Information Control System Installation and Support

SKILLS:**LANGUAGES**

Scripting languages – security design. XML (Extensible Markup Language) security design. ActiveX, applet, servlet security design, Control-SA, Assembler, COBOL, REX/TSO, UNIX, JAVA security design, .NET security concepts (SOA – Service Oriented Architecture)

HARDWARE

Cisco WAN/LAN routers and switches, Foundry Networks WAN/LAN routers and switches, DSL modems, VPN concentrators, IP telephony, NetSys, IDS, TACAS, AVAYA – Definity G2 & G3, Telephone key systems, Lucent Intuity, Siemens HiPath 4000, Xyplex Terminal Servers, Symbol APs – Handheld devices – scanners - bar code readers, LAN Analyzers – SNIFFER, NetXray, Ethereal, TCPDump.

Circuits – T1, ISDN, Frame Relay, PSTN. Hardware encryption accelerator technologies, MQ Series security design, IBM mainframes, Windows based hardware platforms, Unix processors – Solaris, Router appliances – Cisco, Nortel (Passport). Firewall appliances – PIX, TeleWall, Data Tracker, and others.

SOFTWARE

Firewalls: PIX, CheckPoint, Sidewinder, ETM (TeleWall Voice Firewall), NIS (Norton Internet Security), ZoneAlarm, Data Tracker 2700, Microsoft ISA (Internet Security and Accelerator) Server, NetScreen/ScreenOS and NetScreenRemote VPN (Cisco VPN Client), Afaria Mobile Device Management.

Identity Management – IBM Tivoli Identity Manager, RACF.

Anti-virus – McAfee, Symantec – Norton Anti-virus, Trend Micro, Panda, NOD32.

Modem Scanning tools: PhoneSweep, ToneLoc, TeleSweep

Encryption Algorithms: DES, 3DES, MD4, MD5, TLS, SHA-1, AES, Blowfish, Diffie-Hellman(key exchange), EFS (Microsoft Encrypting File System), Omnisecure- VPdisk Pro. PKI solutions. PGP, GPG, SSH, TrueCrypt and other solutions.

Secure Wireless data communications (WEP, WAP, I-MODE, WPA, EAP/TLS)

Scanning tools – NESSUS, NeWT Security Scanner, Nmap, Fpipe, TCPDUMP, Nbtstat, Tracedump, SuperScan, ISS, GFI LanGuard, Harris Stat Scanner, Ethereal, Dumpsec, RAT (Router Audit Tool), OAT (Oracle Auditing Tools), MBSA (Microsoft Baseline Security Analyzer), TigerTools.

IDS – SNORT, Cisco IDS (Net Ranger), TripWire, Veracity

Web testing tools – Empirix (e-Test), Webscarab, OWASP tools, HTTP Sniffer, Nikto.

Biometric authentication solutions such as speech recognition.

TCP/IP V4, LAT, DECnet, SNA, IPX, AppleTalk. Various bridging protocols, Various routing protocols – RIP, IGRP, EIGRP, OSPF, MPLS. SecureOS, AppleTalk, DECNET, SSL - V3, VoIP (Voice over IP – SIP, CoS, QoS, G.711, G.729, H.323), KSH, Bourne Shell, Coldfusion, NCP, VTAM, IIS, Iplanet, WebSphere, WebSphere MQ, WebLogic, E-commerce security design, Intrusion Detection Systems (IDS), SiteMinder – SSO (Single Sign On), ODBC and JDBC security design, Cisco IOS, CiscoWorks 2000, Cisco Secure Policy Manager. TACACS, TACACS+, VPN/IPSEC.

OPERATING SYSTEMS

IBM operating systems such as MVS, VS1, VM and others. DEC – VMS, Solaris, HP-UX, AIX, UnixWare, DOS, Windows NT, Windows 2000, Windows 2003, Windows 2003 Server-DC-AD, Windows XP, Windows XP Professional, Linux/Red Hat, Ultrix, Tandem, S/38, AS400.

DATABASES

Oracle, Sybase, UDB/DB2, Informix, IDMS, Access, SQL Security design, SQL Server 2000, SQL Server 2005.

REGULATORY REQUIREMENTS:

SOX (Sarbanes-Oxley Act of 2002), HIPAA-AS (Health Insurance Portability & Accountability Act of 1996 – Administrative Simplification), DITSCAP (DoD Information Technology Security Certification and Accreditation Process), NIST/FISMA (National Institute of Standards & Technology – Federal Information Security Management Act) C&A (Certification & Accreditation), GLBA (Gramm-Leach-Bliley Act), PCI DSS (Payment Card Industry Data Security Standards).

EDUCATION:

University of Minnesota (late 1960s, early 1970s)

Sioux Falls College: – Accounting/Mathematics. (early 1970s, mid 1970s)

Many and various Technical Training classes, seminars, lectures, certifications as dictated by technology advancements and changes.

OTHER:

Acting Chief Security Officer

TechBios, Inc.

555 North Point Center East

4th Floor

Alpharetta, GA 30022

<http://www.techbios.com/about/team.htm>