

Albert John “A. J.” Wright

7344 Toxaway Drive, Knoxville, TN 37909

Mobile: (865) 388-9951; Email: ajw@ajw.io

Experience

University of Tennessee, System Administration **2012 – Present**

Chief Information Security Officer

Responsible for leading statewide Information Security efforts, setting IT Security strategy, leading IT security governance program, and developing policies, standards, and procedures that provide IT security controls.

- Chaired statewide governance committee for IT Security policy and strategy
- Lead statewide IT services risk assessment and oversight program
- Lead implementation of new program to minimize IT security risks related to PCI Data Security Standard (PCI-DSS) compliance
- Lead deployment of vulnerability management and continuous monitoring programs
- Served on conference board for East Tennessee CyberSecurity Summit

University of Tennessee, University-Wide Administration **2009 – 2012**

Chief Technology Officer and Chief Information Security Officer

Responsible for leading the Information Security efforts and determining technical strategy for Office of Information Technology, the largest IT organization at the University.

- Lead development of long-term research administration software strategy
- Lead deployment of Banner Student Information System web portal
- Lead development of new University-wide IT risk management process based on NIST Special Publication 800 series.
- Lead development of Technical Review Board for determining technology strategy based on technical, business, and customer feedback
- Lead IT industry and legal compliance and risk management for HIPAA Security Rule, PCI Data Security Standard (PCI-DSS), etc.
- Acted as Security Officer under HIPAA security rule for Knoxville Campus

University of Tennessee, University-Wide Administration **2007 – 2009**

IT Security Assessment Team Lead

Responsible for leading team of analysts performing full-spectrum (physical, network, host, etc.) security assessments of systems across the university.

- Worked with executive staff to create university IT Security policies and best practices.
- Lead team that performed first self-assessment of Office of Information Technology
- Developed software to automate, store, and correlate network vulnerability scan information
- Lead development of university-wide enterprise identity management office
- Developed HIPAA compliance plan for management of desktop workstations in Audiology and Speech Pathology Department

University of Tennessee, Knoxville**2005 – 2007***Senior Security Analyst*

Analyst responsible for leading day-to-day operations of the security group at the Knoxville campus. Part of team responsible for full-spectrum (physical, network, host, etc.) security assessments both local and state-wide, forensics, as well as university security policies.

- Implemented ArcSight Enterprise Security Manager software for analyzing and correlating firewall, and IDS/IPS logs.
- Implemented web-based interface to Nessus security scanner for use by user community, including system for supplementing scanner findings with language understandable by non-technical audiences.
- Lead development of workflow for security event response
- Implemented customized web applications for statistic analysis of network baselines

University of Tennessee, Knoxville**1999 – 2005***System Programmer/Analyst and IT Administrator*

Part of team responsible for administration and troubleshooting of the university's central UNIX (Solaris, Linux, AIX, IRIX) servers, with focus on web servers and high-availability SMTP, DNS/DHCP, database, and computation clusters. Partial responsibility for forensic analysis on team-maintained systems.

- Co-authored first UNIX/Linux security policy with Information Security Office.
- Implemented automated Linux system installation that performs system hardening, application configuration, and firewall setup for SMTP and Oracle cluster systems.
- Designed and implemented multi-tiered redundant RFC-compliant SMTP server infrastructure with virus-scanning, spam-scoring, and distributed denial-of-service defense using a local real-time black-hole list to share data across servers and platforms.
- Implemented automated Solaris system hardening scripts that meet or exceed industry and university standards.
- Wrote policy briefs on enterprise storage and Linux system hardening using analysis from Typhon III, Nessus, and other tools.
- Presented papers and tutorials on Sendmail configuration, Solaris system hardening, and SMTP server defense.
- Member of IT Faculty Advisory board

Pellissippi State Technical Community College**1994 – 1999***Computer Technician and System Administrator*

Part of team responsible for maintaining the college's 400+ microcomputer lab systems as well as multi-campus and multi-protocol computer network. Sole responsibility for management of the college's Sun and UNIX servers. Create and maintain in-shop system, script, and application software for UNIX, MS-DOS, Macintosh and VMS systems in C/C++ and appropriate script or batch languages.

- Setup log centralization with NTP-synchronized time stamps.
- Wrote multi-protocol packet analysis tool before TCP-Dump was available. – Wrote software to maintain ideal software state in student labs.

Skills

- Leadership: written and oral communications, experienced public speaker, business process analysis, critical thinking, problem solving, crisis management, ITIL, and systems-analysis skills
- Programming Languages: Java, Perl, C, C++, UNIX Shell Scripting, and SQL
- Operating Systems: Linux, Solaris, AIX, Apple MacOS X, and Microsoft Windows (client and server)
- Applications and Services: Apache (including web technologies such as XHTML, CSS, etc.), MySQL, PostgreSQL, CVS, Oracle, SSH, TCPdump suite, Nessus, WireShark, etc.
- Security: NIST IT Risk Management Framework (Special Publication 800 series), hardware and software firewalls, host-based intrusion detection systems, forensic compromise analysis
- Networking: in-depth knowledge of TCP/IP network protocol suite and packet analysis, Ethernet switches and routers

Education

- University of Tennessee, Knoxville
 - Masters in Business Administration (2010)
 - Funded through scholarship and full-time work
 - Master of Science in Computer Science (2007)
 - Member of CS honor society Upsilon Pi Epsilon
 - Funded through full-time work
 - Bachelor of Science in Computer Science (2004)
 - Member of CS honor society Upsilon Pi Epsilon
 - Funded through full-time work
- Pellissippi State Technical Community College
 - Associate of Arts in Computer Science Technology (1999)
 - Associate of Applied Science in Computer Science Technology (1997)

Certifications

- ITIL Foundation in IT Service Management (2014)
- NAUI Assistant SCUBA Instructor Certification (2013)
- NAUI Master SCUBA Diver Certification (2012)
- NAUI Advanced & Nitrox SCUBA Diver Certification (2009)
- NAUI SCUBA Diver Certification (2009)
- Certified Information Systems Security Professional (CISSP 2008)
- GIAC Securing Oracle Certification (GSOC #0036, 2007)
- GIAC Certified Intrusion Analyst (GCIA #0961, 2005)
- GIAC Cutting-Edge Hacker Techniques (GHTQ #0061, 2005)
- THAWTE Web of Trust Notary (2004)
- SunService Certified Solaris System Administrator (1995)
- A+ Certified Service Technician (1995)
- FBLA State-wide Computer Concepts Competition Winner (1992)
- Earned Eagle Scout Rank, Boy Scouts of America (1991)