

# PAUL D.(DAVE) SUMMITT

MSIA, CISSP, C|CISO, HClSSP, CEH

3712 W Jetton Ave - Tampa, FL 33629

Dave@summitt.net

## Summary of Professional Qualifications

Experienced CISO and EC-Council Certified Chief Information Security Officer, Certified Information Systems Security Professional (CISSP) and former DoD Information Security Officer (ISO) with strong leadership and communication skills. Extensive experience in computing systems, network administration, network security, policies, risk management, compliance, and development of security awareness training programs as well as experience with communicating with board and executive leadership.

## Education

**Master of Science, Information Security**, Computer Forensics Concentration, Norwich University, Northfield, VT

**Bachelor of Science, Information Systems Management**, University of South Florida, St. Petersburg, FL

**Associate of Arts, General Education**, St. Petersburg College, St. Petersburg, FL

**Associate of Applied Science, Electronics Technology**, Wabash Valley College, Mt. Carmel, IL

## Certifications

ISC<sup>2</sup> CISSP #347701      ISC<sup>2</sup> HClSSP      EC-Council Certified Ethical Hacker (CEH)

EC-Council Certified Chief Information Security Officer (C|CISO)

## Awards

2019 TEN-ISE Southeast Executive of the Year nominee

2017 Tech Exec Network (TEN) Information Security Executive (ISE) Southeast Executive of the Year finalist

2017 TEN-ISE Southeast People's Choice Award winner

2017 TEN-ISE North America Executive of the Year nominee

## Membership

Forbes Technology Council

Fellow, Institute of Critical Infrastructure Technology (ICIT)

Florida Infragard, ISC2, ISSA, AEHIS, Tampa Bay Electronic Crimes Task Force.

## Experience

**Moffitt Cancer Center & Research Institute**, Tampa, Florida

**01/2015 – Present**

**Chief Information Security Officer**

Moffitt is the only National Cancer Center designated Comprehensive Cancer in Florida and is currently ranked the number six ranked Cancer Center in the Nation. As Chief Information Security Officer, my responsibilities includes maintaining a Cyber Security program, this process included building and hiring a new security team over the past eighteen months. At present the team is built of 10 personnel and 3 contract positions. The Cyber Security Team is responsible for the organization's Identity and Access management, firewalls, Active Directory, remote access management as well as the proactive monitoring for cyber security events and incident response, performance monitoring of organization's network and applications, and conducting risk assessments. In addition to over-seeing the aforementioned, my direct duties include writing and reviewing Information Technology policy and procedures, presenting Senior-level and board level information on status and recommendations to risks and security plans. Duties also include maintaining team efforts with the legal, compliance and risk management, and human resources departments. Two of the largest initiatives this past year were the implementation of an Identity and Access management process, standup of a Security Operations Center, and beginning a first ever organization wide risk assessment.

Notable accomplishments:

- Standup of a 24/7 Security Operations Center.
- Incorporated Artificial Intelligence in the Security Operations Center
- Joined Fellowship with the Institute of Critical Infrastructure Technology (ICIT)
- Became a member of the Forbes Technology Council
- Participated as a speaker in several Security and Compliance conferences throughout the nation

**UAB Health System.** Birmingham, Alabama  
**Chief Information Security Officer & Corporate HIPAA Security Officer**

09/2013 – 11/2014

As one of the largest employers in Alabama and one of the largest academic medical centers in the nation, its facilities are spread across the state with a central location in Birmingham. The health system averages 50,000 admittances and more than 1.2 million outpatient visits per year. As CISO, the responsibilities included re-structuring the Information Security Program. This process included building and hiring a new security team, reviewing and revising policies, and fostering collaborative team efforts with the legal, compliance and risk management departments. Two of the largest initiatives was the implementation of EHR auditing using FairWarning, the other initiative was conducting 11 Covered Entity organizational assessments by utilizing an in-house data collection tool and the HITRUST Common Security Framework tool.

**Bayfront Health System – Health Mgmt Assoc.** St. Petersburg, Florida  
**Manager, IT Security and Network Services & HIPAA Security Officer**

02/2011 – 08/2013

Bayfront Health is a Level II Trauma center, 480-bed hospital and an academic teaching facility. Bayfront Health system infrastructure is also made up of 6 county-wide Convenient Care clinics, all of which are now part of the Community Health Systems network of 206 hospitals in 29 states. Duties included the responsibility for long-term strategic planning and daily operations of the Network Services and IT Security group. Managed and supported all activities related to the corporate computer systems, network security, and telecommunications network infrastructure. Responsibility included Corporate Compliance with HIPAA, HITECH, as well as other State and Local regulations.

**Advanced Protection Technologies, Inc.** Clearwater, Florida  
**Project Coordinator, Product Development & Engineering Operations**

04/2008 – 07/2010

- Developed test procedures, manufacturing instructions and engineering design and assisted lead engineer in new product development
- Performed a review of the network and computer policies, and information system plans and acceptable use policies.

**Summitt Consulting, llc** Seminole, Florida (Sold business in 2008)  
**President and Owner**

05/1998 – 05/2008

- Supervised and Managed up to 18 people
- Setup site security with SSL certificates, included generation of server keys and registration to Certificate Authorities
- Developed and managed a global helpdesk with over eighteen-thousand users while processing over two-thousand requests per week. Supervised eighteen personnel in six different countries.
- Performed administration, software upgrades, maintenance, backups and support a Unix and Microsoft Infrastructure.
- Provided security server hardening services to various clients.

**Naval Surface Warfare Center** Crane, Indiana  
**Technical Representative, Naval Sea Systems Command IW6**

10/1984 – 06/2005

- Served as Automated Data Processing System Security Officer (ADPSSO) and Contracting Officers Technical Rep
- Held Government signature authority for review and approval of hardware and software requirements, system security specifications, and prime item development specifications
- Held Data and Configuration Manager positions on three military projects
- Established and provided Project Management on Computer Repair Program that resulted in Government savings of over \$1.2 million annually
- Served as Navy's Cooperative Engagement Capability (CEC) program Technical Representative
- Led migration, upgrades, and testing for various revisions of military software and hardware
- Participated in Award Fee boards, Failure Analysis, Risk Assessment, software working groups
- Provided software upgrades, support, server and network administration, security monitoring, data backup and restoration on several Navy networks and servers
- Provided Acceptance Testing of software and hardware equipment and systems on numerous DoD projects