

**Harvey Newstrom**  
CISSP CISA CISM CGEIT CSSLP CRISC CIFI NSA-IAM ISSAP ISSMP ISSPCS IBMCP  
Melbourne, FL and Washington, DC  
Updated: 3/1/2011

mail@HarveyNewstrom.com  
www.HarveyNewstrom.com  
301.681.8704  
321.574.1212

### Professional Profile

Harvey Newstrom is a recognized security leader who specializes in helping Fortune-500 corporations and Federal Agencies establish world-class security programs. These programs serve not only to protect organizational assets, but to increase mission efficiency and effectiveness in a global environment. Mr. Newstrom combines executive business savvy with technical know-how to produce strategies that are both achievable and optimal. The diversity of his consulting portfolio with industry, military, and government clients gives him more practical experience with real-world threats than most security professionals. Mr. Newstrom has authored hundreds of white papers, dozens of technical manuals, and given countless lectures throughout his career.

### Consulting Portfolio

Mr. Newstrom cofounded Newstaff, Inc., a security consulting company with customers in both government and industry. He helped develop intellectual capital used by IBM's Security and Privacy consulting practice. He helped establish the Ethical Hacking division for Fiderus, a \$75 million security consulting startup. He designed the security architecture used by the National Archives and Records Administration and led the security teams that fulfilled the last two five-year contracts of that security program. His work for the federal agency was praised by OMB and later requested by NIST for use in improving federal security standards for all agencies. He has established security programs for dozens of Fortune 500 companies and has helped operate and improve security programs for a dozen federal agencies.

### Active Clearances

**TS/SCI – Top Secret / Sensitive Compartmentalized Information (3/21/2008)**  
**TS – Top Secret (8/15/2007)**  
**S – Secret (8/5/2005)**  
**SSBI – Single Scope Background Investigation (3/7/2007)**  
**NACI – National Agency Check and Inquiry (CIA, DoD, DoJ, FBI, IRS, NRO, NARA, NIST, NSA, USDA)**

### Current Certifications

**CRISC #1000261 – ISACA Certified in Risk and Information Systems Control (6/22/2010)**  
**CSSLP #26730 – (ICS)<sup>2</sup> Certified Secure Software Lifecycle Professional (4/8/2009)**  
**CGEIT #801400 – ISACA Certified in the Governance of Enterprise IT (12/11/2008)**  
**ISSPCS #8 – International Systems Security Professional Certification Scheme (6/1/2005)**  
**CIFI #115 – IISFA Certified Information Forensics Investigator (4/12/2005)**  
**ISSMP #26730 – (ICS)<sup>2</sup> Information Systems Security Architecture Professional (9/7/2004)**  
**ISSAP #26730 – (ICS)<sup>2</sup> Information Systems Security Management Professional (8/31/2004)**  
**CISA #332168 – ISACA Certified Information Systems Auditor (9/16/2003)**  
**CISM #300730 – ISACA Certified Information Security Manager (5/29/2003)**  
**NSA-IAM #20021016 – National Security Agency Infosec Assessment Methodology (10/16/2002)**  
**CISSP #26730 – (ICS)<sup>2</sup> Certified Information Systems Security Professional (11/2001)**  
**IBMCP #19991001 – IBM Certified Professional consulting in Security and Privacy Services (10/1/1999)**

### Relevant Training

**Federal CSAM – Dept. of Justice Cyber Security Assessment and Management Training (3/30/2010)**  
**EnCase Forensics – Guidance Software EnCase Forensics Training Course (5/22/2009)**  
**NetForensics – NetForensics SIM-One Training Course (5/29/2008)**  
**CMMI Level 3 – Capability Maturity Model Integration training and team lead experience (5/12/2006)**  
**DNI DCID 6/3 – DNI Special Security Center DCID 6/3 Training (4/5/2006)**  
**SANS GSEC #2137 – SANS GIAC Security Essentials Certification (9/2002, 10/2004, 10/2006, expired 10/2008)**  
**IBM PM – IBM Project Manager Training (2/2000)**  
**Harris Executive – Harris Executive Leadership Training (714/1989)**

### Education

**Bachelor's Degree – Bachelor of Professional Studies, Barry University, 3.692GPA (9/16/1989)**  
**Associate's Degree – Associate of Science in Computer Science, Morris Junior College, 4.0GPA (6/29/1984)**

## **Relevant Skills and Expertise**

**Skills:** Confidentiality, Integrity, Availability, Access Control, Awareness and Training, Audit and Accountability, Certification and Accreditation, Testing, Penetration Testing, Beta Testing, Compliance Testing, Vulnerability Scans, Ethical Hacking, Appraisal, Risk Assessment, Forensics, Investigations, Configuration Management, Security Maintenance, Contingency Planning, Strategy, Development, Design, Identification and Authentication, Architecture, Standards, Policies and Procedures, Implementation, Remediation, Firewalls, Intrusion Detection Systems, Incident Response, Media Protection, Physical Security, Environmental Security, Network Security, System Security, Personnel Security, Consulting, Public Speaking, Research and Development, Organizational Change, Security Program Management, Organization Effectiveness.

**Industries:** Fortune-500, Military, Government, International, e-Commerce, Consulting, Business, Education, Entertainment, Financial, Healthcare, Internet, Manufacturing, Non-Profit, Publishing, Technology, Utilities.

**Standards:** ACM, BS-7799, CBK, CC, CISA, CIA, CGEIT, CIFI, CISA, CISM, CISSP, Clinger-Cohen, CMM, CMMI, CNSSI, COBIT, CRISC, DCID 6/3, DITSCAP, DoD, DoD 5015.2-STD, DoJ, E-Government Act, EFF, FEA, FBI, FIPS, FISCAM, FISMA, GAO, GLBA, HIPAA, IAM, IBM, IEEE, INFOSEC, ISACA, (ISC)<sup>2</sup>, ISSAP, ISSMP, ISSPCS, ISSA, ISO-15489, ISO-9126, ISO-9000, ISO-17799, ISOO, ITRMA, ITSEC, NARA, NCIC, NIACAP, NISPOM, NIST, NISTIR, Orange Book, OMB, PCI, Privacy Act, RFCs, SANS, Sarbanes-Oxley, SAS-70, SSE-CMM, TCSEC, USDA, US Law, and others.

## **Career History**

**Principal Security Architect**, Science Applications International Corporation, Lanham, MD (4/2004 – present)

Security Program Lead on two consecutive five-year contracts to implement a federal agency security program for the National Archives and Records Administration (NARA). Transformed the security program from CMMI Level 1 to become certified at CMMI Level 3 in 2006 with plans to attempt CMMI Level 5 certification later this year. Developed the agency security architecture to establish security policies and security requirements for the agency. This agency architecture was later praised by the federal Office of Budget and Management (OMB) as the best security architecture submitted by a federal agency. It was also officially requisitioned by the National Institute of Standards and Technology (NIST) for use in improving federal requirements for all agencies.

Founded agency risk boards and risk review processes. Founded agency steering committees and technical design review committees. Published annual security program plans to guide the security program each year. Published white papers, methodologies, security technical implementation guides (STIGs), and templates to standardize and regulate agency security activities. Lead teams to develop and administer the agency's annual security awareness program and more advanced security training programs. Established the agency security portal to provide all security tools and security documentation via a single web site.

Established security assessment teams and standards to perform certification and accreditation (later migrated to assessment and authorization) activities for 41 systems and a dozen general support systems providing common security controls for the agency. Participated in business continuity and disaster recovery initiatives. Worked with engineering teams to ensure that technical designs and operational implementations met security requirements. Established and lead monitoring teams using various monitoring tools, both for intrusion detection and operations performance. Established incident response teams and procedures to respond to security incidents. Lead teams performing audit response activities to provide compliance assurance.

**Principal Security Consultant**, Newstaff, Melbourne, FL (1/2001 – 04/2004)

Returned to Newstaff to lead a security transformation initiative for Fleming Companies, Inc. Designed a completely new architecture to modernize the organization security, including migrating token-ring LANs to Ethernet LANs, migrating frame relay WANs to ATM, migrating Bay Networks routers to Cisco routers, and migrating IBM firewalls to Cisco firewalls. Simultaneously established a new security program to manage the new infrastructure by interviewing and hiring new security staff, establishing new security policies, and initiating security monitoring, security training, and incident response capabilities. Also performed add-on work to coordinate the security portion of a merger between Fleming and K-mart, by merging the existing K-mart security operations into the new Fleming security program.

Other projects at Newstaff included developing automated security tools, security consulting methodology, and performing independent research in security. Wrote proposals, generated sales, and acted as project manager on all security projects. Provided the expertise, training, methodology, and direction for all security consultants. Acted as project manager for security consulting projects. Lead Newstaff consulting projects for the IBM, Advantis, AT&T, Philips Electronics, Mayo Clinic, Deloitte & Touche, Ryder, Fleming, K-mart, County of Hillsborough, Sykes, Ultimate Software, TEKsystems, CGI Systems, Computer Horizons Corporation, and Llewellyn Publishing.

**Director of Security Testing**, Fiderus Strategic Security and Privacy Services, Cary, NC (8/2000 – 12/2000)

Created the Security Consulting Practice of “ethical hackers” for this \$75 million startup. Led my division to win the company’s first contract. Led the company in sales during the first quarter. Developed methodology for security testing, penetration testing, and auditing. Conducted training classes for consultants, both for my division and other divisions. Established a beta-test lab with penetration testing tools during the first quarter. Delivered an operational and profitable consulting practice to the company in just four months.

**Lead Security Consultant**, IBM Security and Privacy Services, Orlando, FL (7/1998 – 8/2000)

After consulting via my own company to IBM for a few years, and assisting with the proof-of-concept for IBM’s new Security and Privacy Services practice, IBM hired me directly to lead teams and develop methodology for the new practice. One of these methodologies was submitted for a patent during my first year with IBM. I lead IBM teams in establishing security programs for 1998 and 2000 Olympics, JPMorgan, Chase Manhattan, Reliant Energy, Bank of America, and FirstUSA Bank. I lead IBM teams in transforming security programs for Staples, ADP, Credit Suisse First Boston, EBS, Anthem, and Florida Power & Light. I lead the national practice in follow-on contracts for my consulting work. Also lead teams for internal IBM product development and conducted classes for IBM developers on secure software development and testing through all phases of system development lifecycle.

**Lead Security Consultant**, Newstaff, Melbourne, FL (1/1995 – 7/1998)

Cofounded Newstaff in 1995 to provide mission-based security architecture and security program consulting services to Fortune-500 companies and government agencies. Wrote proposals, generated sales, and acted as project manager on all security projects. Provided the expertise, training, methodology, and direction for all security consultants. Landed the company’s first account, which was a six-month contract with IBM, leading to a total of six IBM contracts. Traced unexplained campus-wide computer shutdowns at IBM’s famous Boca Raton site to a design flaw in the NetBIOS protocol. IBM redesigned part of the NetBIOS protocol specifications based on my analysis. Reorganized South Florida campus from one big site into five distributed sites. Helped establish proof-of-concept for IBM’s new Security and Privacy Services practice. Automated network monitoring, intrusion detection, and security alerts for IBM South Florida security operations.

**Lead Engineer**, Harris, Palm Bay, FL (9/1990 - 12/1994)

Appointed first Information System Security Officer (ISSO) for Harris Electronic Systems. Established policies and procedures to define the new position. Manager for security R&D teams and security engagement teams for classified projects. Project Manager for internal security projects and external customer security engagements. Certified software and servers for internal production use. Wrote in-house security standards, policies and procedures. Chaired change-control committee, design-review teams, and organizational steering committees.

**Senior Engineer Specialist**, Harris, Palm Bay, FL (9/1989 – 8/1990)

Lead in-house R&D in network security. Developed system software and tools for security testing, monitoring, reporting, analysis, and secure communications. Managed all phases of system development lifecycle. Operated company beta-test lab to evaluate products before shipping. Certified software and servers for internal production use. Wrote in-house security standards, policies and procedures. Chaired change-control committee, design-review teams, and organizational steering committees.

**Engineer Specialist**, Harris, Palm Bay, FL (9/1987 – 8/1989)

Developed system software and tools for security testing, monitoring, reporting, analysis, and communications. Managed all phases of system development lifecycle. Wrote in-house security standards, policies and procedures. Chaired change-control committee, design-review teams, and organizational steering committees.

**Programmer**, Harris, Palm Bay, FL (1/1985 – 8/1987)

Developed system software and tools for security testing, monitoring, reporting, analysis, and secure communications. Managed all phases of system development lifecycle.

**Lead Software Engineer**, Castronova Enterprises, Melbourne, FL (2/1983 - 8/1984)

Managed a small team of developers to produce secure turnkey systems for industry. Managed security in all phases of system development lifecycle. Performed design review, monitored development, performed acceptance testing, and audited client implementations.