

Richard F. Forno
7716 Effingham Square
Alexandria, Virginia 22315-5917
USA
rforo@krvw.com

Technical Skills

UNIX, Linux, Windows, TCP/IP, Computer Forensics, Incident Response, Penetration Testing, Security Management and Operations, Critical Infrastructure Protection.

Summary

Mr. Forno is a career security technologist specializing in security program development, incident response, training, and network security operations for large government and commercial organizations. A frequent lecturer, he is also the author of several security whitepapers, many articles, and co-author of the security books *Incident Response Planning & Management* and *The Art of Information Warfare*.

Work Experience

2005 to Present - KRvW Associates, Principal Consultant
(DoD Clearance info available on request)

Responsibilities include:

- *Consulting services*, including: Incident Response planning and emergency operational support; Intrusion monitoring systems design, review, and deployment planning; IT security process and design reviews; IT security technology decision support; firewall/secure network design and review; threat assessments and related strategic security support activities.
- *Training services*, including: 1/2 day through 2 1/2 day seminars on Incident Response, Threat Awareness, and other security topics.

2004 to 2005 - Gartner Inc, Enterprise Risk Management, Associate Director

Assisted in the development of the firm's information assurance consulting offering. This effort included providing direct strategic advisory services to Fortune 500 firms in the areas of disaster recovery, critical infrastructure protection, enterprise identity management, network vulnerability analysis, and incident response.

2001 to 2004 - Independent Security Consultant

Major activities included:

- Assisted several start-up ventures, including serving as interim Chief Technology Officer for a Herndon, VA-based government IT security solutions provider.
- Served as lead information assurance engineer for a specialized IO/C3I program for the Department of Defense.
- Conducted both paid and pro-bono senior-level research, advice, publication, and lecturing on information warfare, critical infrastructure protection, privacy, and information assurance policy issues to commercial, academic, and government clients, including the Navy's Critical Infrastructure Protection Program Office, Joint Task Force (Computer Network Operations) and the Chief of Naval Operations Strategic Studies Group.
- Penned a recurring column for Securityfocus.Com from 2001-2003.
- Co-founder and technical director of a large nonprofit distribution network for the timely delivery of

unclassified news and intelligence analysis serving the US government, military, and emergency response communities; the service was recognized for its utility during 09-11-01 and subsequent ongoing military operations.

- Conducted monthly lectures on information warfare and critical infrastructure protection at the National Defense University in Washington, DC from 2001-2003.
- Served as faculty subject matter expert and founding member of the Academic Advisory Board of the Northern Virginia Community College Information Security Degree Program.

1998 to 2001 - Chief Security Officer, Network Solutions, Inc. (InterNIC)

Responsibilities included:

- Development and management of an enterprise information assurance program and all related processes, budgets, and personnel.
- Lead incident response and investigative activities, including those related to litigation support.
- Ensure and continually enhance the security of the InterNIC and Internet Shared Registry Systems.
- Conduct network and facilities vulnerability and penetration testing, and technical due diligence activities in support of corporate acquisitions.
- Serve as the company's security subject matter expert to visiting Members of Congress, industry leaders, and the information security community.

1995 to 1997 - U.S. House of Representatives, Senior Security Analyst (HS-9)

Responsibilities included:

- Investigated Internet attacks against the House, conducted computer forensics on seized equipment, developed security policy, and served as technical liaison for interagency investigations.
- Developed and presented various policy briefings for Congressional Offices. Assisted in the development of the House Information Security Reference, a multi-volume Information Security Policy and Oversight publication.
- Facilitated creation of the House Computer Emergency Response Team (USHCERT) and the team's membership into the Forum of Incident Response Security Teams (FIRST).
- Served as technical advisor and coordinator for the deployment of a standard encryption system for the House and Library of Congress.

1992 to 1995 - Assorted Technical Support and Network Administration Activities

For the U.S. House of Representatives Office of Legislative Counsel...

Managed Novell 3.12 and Windows NT LANs and provided user support as needed for the nation's senior-most legislative drafting organization, ensuring 24x7 uptime for all legislative information systems; Developed systems access policy and implemented security measures; Established first full Internet connection and public web site for the office; Supervised and coordinated vendor and staff activities for major network upgrades, including a large-scale network migration from Netware 3.12 to NT 4.0 on-time and under-budget; Developed material and conducted user training for office applications; Developed and implemented security protocols for office networks to exchange information with US Senate and GPO clients.

For a Virginia-based defense contractor...

Maintained and provided real-time field support for Army Corps-level C2I systems running the Automated Deep Operations Coordination System (ADOCS) providing extensive fire planning, coordination, and execution, data display and communications capabilities (including realtime data sharing) among multiple workstations across multiple Services and user organizations in joint and combined military environments; Provided simulations and testing support for the Defense Intelligence Agency FULCRUM system used for intelligence, targeting, operations and planning and assisted in product revision of the Surrogate Travel/SITETOUR system (STS) in support of Army Special Operations activities.

For the Washington College of Law...

Provided assorted Unix, Novell and Windows-based system administration, technical support and help desk activities for the American University Law School, including serving on AU and Novell's beta test team for Netware 4.0 in an enterprise environment.

Publications and Related Experience

- **Books & Articles:** O'Reilly's *Incident Response Planning & Management* (2001); *The Art of Information Warfare* (1999); *Weapons of Mass Delusion* (2003). Contributor, *Cyberwar 2.0, Myth, Mystery, Reality* AFCEA Press (1998). Several white papers and current technology commentary at INFOWARRIOR.ORG (some currently used as US government training resources.) Commentaries and op-eds appear in many national and international news sites, including News.Com, Wired, The Register, Sydney Morning Herald, and others.
- **Academic Publishing:** *PKI: A Matter of Trust and Value* (Co-Author, Excerpt appears in Inside Risks 132, CACM 44, 6, June 2001); *Applying the Intelligence Preparation of the Battlefield Process to Network Incident Response* (Co-Author, International Journal of Computer and Telecommunications Networking (Vol. 34 (4) (2000) pp. 671-697.)
- **Outreach/Speaking:** Frequent speaker at law enforcement, industry, academic, and intelligence community conferences and seminars. Participant on the 2000 White House task force studying INFOSEC Education as part of the President's Critical Infrastructure Security Program Initiative.
- **Affiliations:** Director, G2-Forward (co-founder and technical director); Executive Advisory Board Member, Symbiot and St. Bernard Software; Past President, Potomac Chapter, National Military Intelligence Association; Member, High Technology Crime Investigators Association; Past Director and OPSEC Journal Editor, Operations Security Professionals Society.

Education

2008: PhD Candidate, Curtin University of Technology

2002: M.A., Salve Regina University

1997: Certificate in National Security Studies, US Naval War College

1994: B.A., American University

1992: A.B., Valley Forge Military College

Completed assorted information and operations security courses offered by the National Security Agency and attended the USAF Office of Special Investigations Basic Computer Crime Investigations Course in 1996.