
Erick Rudiak

INFORMATION SECURITY LEADER

Data and Application Security • Technology Risk Management • Internet Application Architecture

Regularly consulted with **clients' security officers and firm executives**, defining and articulating corporate Information Security posture and mapping it to clients' needs and priorities. Formulated, published, implemented, and enforced corporate **technology risk management methodology**, encompassing all areas of technology and application development. Corporate **Leadership Group** and **Technology Governance Board** member since 2006. **Global responsibility** for corporate network infrastructure security of HR Outsourcing and Consulting firm with \$2.9B in annual revenue, over 24,000 employees and over 100 offices worldwide. **Ten years of experience** cultivating and leading a highly technical team, incorporating analytical, operational, research and development, and vulnerability assessment skills. Championed best-of-breed open source technologies to construct scalable network security platform, resulting in **over \$1M savings** over equivalent commercial offerings.

CORE COMPETENCIES

- Team Leadership
- IP Networking
- Strategic Technology Planning
- Security Policy Development
- Technology Risk Management
- UNIX
- Vulnerability Management and Assessment
- Security Metrics
- Internet Application Architecture

PROFESSIONAL EXPERIENCE

Hewitt Associates – Lincolnshire, IL

1993 - Present

Deputy Chief Information Security Officer (2007 -)

Responsible for four groups, totaling 18 associates, providing security governance, client relationship management and technology risk management for corporation.

Key Achievements:

- Defined security risk management strategy for high-profile corporate mergers and acquisition activity.
- Defined LAN security roadmap, incorporating VoIP, closet switch, and wireless security.
- Designed corporate risk dashboard, incorporating evergreening and collaborative editing of policy documents and calibration of security metrics to critical business measures.
- Led deployment of application firewall technology to protect mission-critical web infrastructure from zero-day attacks.
- Managed budget of over \$5M in capital and operational expenditure on security.

Network Security Manager (1999 – 2007)

Led and managed team, totaling 20 associates globally, with responsibility over network security infrastructure, research and development, and vulnerability assessment disciplines.

Key Achievements:

- Authored corporate-wide network security policy.
- Established vulnerability assessment practice, proactively ensuring safety of client-facing applications and minimizing client audit findings.
- Maintained consistent security posture while engineering integration of corporate network through the course of six mergers and acquisitions.
- Maintained minimal turnover in highly technical group (20 adds, 3 departures in 8 years).
- Adapted and expanded network edge design to support new multi-process outsourcing business model.
- Designed and maintained Internet edge and DMZ infrastructure supporting flagship customer-facing applications, incorporating best-of-breed commercial and open-source technologies to deliver defense-in-depth security while maintaining high throughput and availability.
- Spearheaded use of TLS for encrypted delivery of corporate electronic mail across public networks.
- Defined and executed spam reduction strategy, lowering overall SMTP spam volume by more than 50%.
- IS Leadership Team member since 2004.

Network Security Architect (1997 – 2007)

First full-time network security engineer at Hewitt; designed and implemented secure, repeatable network connectivity model for 200+ private intercorporate IP connections.

Key Achievements:

- Developed custom workflow engine for firewall change management, enabling auditable revision control and peer review for all policy and configuration updates.
- Developed, deployed, and maintained secure centralized management and monitoring methodology for 300+ Solaris- and OpenBSD-based proxy and stateful inspection firewalls. Use of open source technologies currently results in over \$1M annual cost savings.
- Audited and evaluated security risks in corporate networks, commercial applications, and internally-developed web sites.
- Promoted, defined, and enforced secure application coding practices.
- Developed utility and methodology for auditing superuser access to critical systems, facilitating SOX compliance.
- Developed, deployed, and maintained cross-platform intrusion reporting system.
- Established and enforced the use of sudo and SSH as corporate standards for UNIX system access and management.

UNIX Systems Architect (1993 – 1997)

First full-time UNIX system engineer at Hewitt.

Key Achievements:

- Converted flagship MVS-based OLTP application to run on Pyramid DC/OSx using UNIKIX, Oracle, and a Solaris-based SNA gateway, demonstrating mainframe-to-UNIX portability.
- Architected Internet-based delivery model that enabled self-service access to flagship benefits recordkeeping application.
- Established UNIX Technology group, growing from one person in 1993 to three in 1997.
- Responsible for supporting 50+ Solaris, AIX, Pyramid, and Siemens-Nixdorf UNIX servers.

TECHNICAL BACKGROUND

Platforms: Solaris, OpenBSD, Windows, Linux

Technologies: Apache, mod_security, BIND, sendmail, BigIP, 3DNS, cricket, RRDTool, Wireshark, tcptrace, sudo, cfengine, snort, samhain, squid, IPFilter, Nessus, CORE Impact, amap, nmap, pmwiki

Languages: UNIX Shell, awk, C

Education: Bachelor of Science in Electrical Engineering
Northwestern University

1993
Evanston, Illinois