

# Erick Rudiak

---

## INFORMATION SECURITY LEADER

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

---

**Chief Information Security Officer** for \$3.2B global company with over 28,000 employees and over 100 offices worldwide. **Global responsibility** for all data and systems security, protecting over 100M records of Personally Identifiable Information, executive compensation, merger and acquisition planning, and proprietary corporate data. Regularly consults with clients' and suppliers' executives and data protection leaders, 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. Thirteen years of management 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

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

---

### PROFESSIONAL EXPERIENCE

**Hewitt Associates** - Lincolnshire, IL

1993 - Present

#### **Chief Information Security Officer (2007 - )**

Responsible for three functional groups, totaling 10 associates, providing global information security governance, policy development, security metrics, and overall technology risk management for global corporation.

#### *Key Achievements:*

- Defined corporate information security strategy and guidelines for mergers, acquisitions, and divestments.
- Established regular risk register reviews with VP's and CTO's of key business segments while standardizing delegation of authority, reporting, and risk acceptance processes. Authored monthly "strategic security insights" series for CIO's Global Technology Leadership Team.
- Established and led security champions programs in Information Technology and Application Systems, creating career pathing, responsibility for data security, and consistent line of sight between three separate organizations.
- Authored and published global corporate information security policy, coordinating regional deployment and awareness for European and Asian operations. Pioneered use of wiki technology to maintain transparency and evergreening of policy documentation.
- Established security metrics program and Client Security Concern Index. Participant and contributor to the Center for Internet Security's Consensus Security Metrics project.
- Led deployment of web application firewall technology to protect mission-critical web infrastructure
- Led deployment of secure endpoint inspection for remote workforce.
- Steered deployment and governance of data leakage prevention tool to over 14,000 desktops.

- Steered global deployment and governance of wireless intrusion detection technology.
- Managed budget of over \$3M in capital and operational expenditure on security technologies.
- Partnered with Chief Privacy Officer to standardize contractual security exhibit for clients and suppliers. Regularly reviewed contracts for compliance, risk, and liability.
- Global Technology Extended Leadership Team member

### **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.
- Defined network access security roadmap, incorporating VoIP, closet switch, and wireless security.
- 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 volume by more than 50%.
- Architected and deployed two-factor authentication solution for firewalls, network devices, and UNIX platforms
- IS Leadership Team member since 2004.

### **Network Security Architect (1997 - 2007)**

First 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. Extensive use of open source technologies resulted in over \$1M annual opex 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 UNIX system engineer at Hewitt; established platform architecture standards, deployed and supported mission-critical transactional, networking, and reporting applications.

#### *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 benefits recordkeeping application for 1 million participants.
- 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, Verdasys Digital Guardian, milter-greylst, RSA SecurID, pam\_radius, Paros

**Languages:** bourne shell, awk, C

---

## EDUCATION

**Northwestern University** Evanston, Illinois

Bachelor of Science in Electrical Engineering

1993