Erick Rudiak

erick.rudiak@gmail.com
https://erick.rudiak.com/ciso/
https://linkedin.com/in/erickrudiak

CISO & Technology Leader

Chief Information Security Officer (CISO) for $100B+ pharmacy benefit manager and $4.5B+ worldwide leader in HR outsourcing. **Global responsibility** for all data and systems security, protecting over 160M records of sensitive, personally identifiable information and corporate intellectual property. **Trusted advisor** to CEOs, Boards of Directors, executive committees, CIOs, CTOs, CPOs, and GCs. Valued for thought leadership, technical acumen, and **business-positive approach** to managing risks to information. **Over twenty years of experience** leading high-performing technical and non-technical teams. Strong track record of **attracting and developing top talent** to succeed in executive roles. Core competencies include:

- Enterprise risk management
- Security policy development and enforcement
- Cyber risk assessment & threat modeling
- Strategic technology planning
- Breach resistance and controls assurance
- Information Security metrics and program maturity
- Internet Application Architecture
- Quantitative risk assessment and decision science

Career Chronology

Express Scripts
Saint Louis, MO

Vice President & Chief Information Security Officer 2012 –
Senior Director & Chief Information Security Officer 2011 – 2012

Responsible for enterprise-wide Information Risk Management (IRM) program at largest U.S. pharmacy benefits manager, leading team of ~150 (employees + contractors). Accountable for all enterprise data protection, including information security policy and strategy, digital forensics, incident response, cyber threat intelligence, supplier risk management, client audit and go-to-market support, vulnerability management, business continuity, disaster recovery, subsidiary risk, regulatory compliance, controls assurance, crisis management, and attack simulation.

Highlighted accomplishments:

↗ Advised Senior Staff and Board of Directors quarterly on program health and industry threat landscape;
↗ Established and matured Digital Forensics & Incident Response practice, improving time-to-discover and time-to-close for potential security events by >75%;
↗ Defined and executed robust and flexible security models and detailed assessment playbook for multiple mergers ($29B and $69B) and acquisitions ($0.25B and $3.5B);
↗ Reduced breach loss ceiling by >$100M through institution of aggressive data retention schedules;
↗ Defined and evolved enterprise crisis response playbook, leading cross-functional tabletop exercises and training senior leaders (CEO, CFO, GC, CMO, SVP Sales, CIO, COO, etc.) on roles and responsibilities;
↗ Adapted information risk management practices into company-wide adoption of Agile
↗ Defined and executed company strategy for attaining SOC2 certification
↗ Influenced strong, company-wide security culture through “just-in-time” awareness program, delivering

automated corporate document classification and reducing high-risk employee Internet usage by >60% while improving voluntary reporting of phishing attacks by a factor of >10x;
- ↗ Partnered with Procurement to deliver 71% reduction in supplier contracting risk while absorbing >30% annual growth in vendor portfolio;
- ↗ Architected and delivered refresh of Data Theft Prevention program, resulting in >50% reduction in high-risk external data transmission by employees, and supporting successful prosecutions of multiple insider threats to company brand and trade secrets;
- ↗ Chaired enterprise-wide Information Protection Steering Committee, aligning senior stakeholders from HR, Sales, Legal, Operations, Compliance, and IT;
- ↗ Directed cost-effective process and technology improvements, reducing endpoint attack surface by >90%;
- ↗ Delivered 59% improvement in patient password security through application of behavioral health science;
- ↗ Established Client & Supplier Risk Management practice, aligning with Sales & Account Management, Corporate Procurement, and Vendor Management organizations;
- ↗ Introduced Red-Team/Blue-Team attack simulation program to validate enterprise defense effectiveness;
- ↗ Established application security practice, incorporating threat modeling and secure coding best practices into enterprise SDLC and project management lifecycles;
- ↗ Launched cross-functional Security Champions organization, creating career paths in security for technologists, and coordinating activities across IT operations, architecture, engineering, and development;
- ↗ Automated on-boarding and security entitlement review processes, yielding >90% productivity improvement;
- ↗ Partnered with Fraud, Waste, and Abuse department to improve heuristic detection of insider threats;
- ↗ Designed and delivered enterprise information security risk register and scorecard;
- ↗ Expanded business continuity coverage for all North American sites while reducing 3-year costs by >$1M;

Hewitt 2007 – 2010
Lincolnshire, IL

Chief Information Security Officer

Responsible for global, enterprise-wide Information Security program, protecting PII for over 16M plan participants, and enterprise IP of $4.5B global enterprise with presence in 37 countries. Led team of 17 associates globally, providing information security governance, client relationship management, infrastructure and application security, policy development, security metrics, and overall technology risk management.

Highlighted accomplishments:

- ↗ Defined corporate information security strategy and guidelines for mergers, acquisitions, and divestitures;
- ↗ Authored and published global corporate information security policy, coordinating regional deployment and awareness for European and Pacific Rim operations;
- ↗ Pioneered use of wiki technology to deliver transparent, evergreen policy documentation;
- ↗ Led deployment of application firewall technology to protect mission-critical web infrastructure;
- ↗ Steered deployment and governance of data leakage prevention tool to over 14,000 desktops;
- ↗ Partnered with Chief Privacy Officer to standardize contractual security exhibit for clients and suppliers, regularly

reviewing contracts for compliance, risk, and liability.

Hewitt 1999 – 2007

Director of Network Security

Led global team of 20 FTEs, responsible for all network security and vulnerability assessments. Spearheaded use of TLS for secure delivery of inter-corporate messaging. Established application security assessment practice and SDLC. Delivered open-source spam reduction solution, resulting in >70% drop in volume. Architected multi-factor authentication solution for critical infrastructure.

Hewitt 1997 – 1999

Network Security Lead Architect

Designed and implemented secure, repeatable network connectivity model for 200+ private inter-corporate connections. Developed custom workflow for firewall change management, enabling auditable revision control and peer review. Architected open source firewall strategy, resulting in over $1M annual run-rate savings. Assessed security risks in corporate networks, commercial applications, and internally-developed websites. Defined corporate information security standards.

Hewitt 1993 – 1997

UNIX Systems Lead Architect

Established, deployed, and supported platform architecture standards. Led conversion of flagship MVS-based OLTP application, demonstrating mainframe-to-UNIX portability. Architected Internet-based delivery of self-service 401k plan management for over 1M participants.

Additional Professional Experience

Center for Internet Security (2010): Contributor to baseline security metrics working group.

HITRUST (2011 - current): Executive board member and conference speaker/panelist.

EC Council (2013): Keynote speaker at 2013 CISO Summit.

Cybersecurity Workforce Alliance (2015): Advisor to working group defining skills assessment model for students matriculating from undergraduate cybersecurity programs.

Technical Competencies

Platforms: Linux, Windows, OpenBSD, Solaris

Protocols: TCP/IP, HTTP, DNS, SMTP

Tools: Apache, mod_security, Websense DLP, F5 load balancers, cricket, dnscat2, Wireshark, sudo, cfengine, ipfilter, FreeBSD pf, nmap, Burp suite, milter-greylist, SecurID, netflow, etc.

Education

Northwestern University — Evanston, Illinois
Bachelor of Science in Electrical Engineering — December 1993

Carnegie Mellon University Heinz College — Pittsburgh, Pennsylvania
Chief Risk Officer Certificate — January 2018