

Larry J. Hughes, Jr.

curriculum vitae

larry.hughes@infosecintrospect.com
www.infosecintrospect.com
voice: (206) 930-4282

7820 SE 71st St.
Mercer Island, WA 98040
fax: (206) 230-0721

Qualifications

Security expert, architect and consultant. Former head of Amazon.com's worldwide information security team. Author of a pioneering and acclaimed Internet security book. Leader of corporate compliance efforts, e.g. PCI/DSS, Sarbanes-Oxley 404. Member of technical advisory boards. Speaker at national, regional and local events. Skilled navigator of competing business and technology needs and requirements.

Positions

Infosec Introspect, Inc.

Founder and Chief Ruminator (2006-Present)

Information security consultant for businesses of all types and sizes. Foci of practice are:

For Businesses: Making the business case for security. Improving the overall security posture. Producing business-compatible and -palatable security requirements. Defining and tracking security metrics. Meeting and exceeding best practices. Architecting applications and infrastructure for long-haul stability, scalability and security. Publishing and enforcing sane security policies. Achieving regulatory and industry compliance. Minimizing outsourcing risks in pragmatic ways. Assessing technology risks associated with acquisitions and spinoffs. Provoking and holding security mindshare within the enterprise

For Venture Capital Firms: Assessing fund-worthiness of tech startups via staff interviews, assessments of blueprints and intellectual property, surveys of competitive landscapes. Recommending changes to strategy and roadmap. Identifying untapped market sweet spots.

For Startups: Technical advisory. Reconciling rapid growth and security. Planning for regulatory and industry compliance without derailing the business.

For Product Vendors and Service Providers: Positioning and messaging to attract world-class customers. Anticipating and understanding customers' compliance and other security requirements. Architecting for long-haul stability, scalability and security. Identifying untapped market niches. Building effective roadmaps.

Advisory Board Memberships

Vantos ♦ www.vantos.com (2007-Present)

SiteScout ♦ www.sitescout.net (2007- Present)

Semplice ♦ *stealth mode* (2007 - Present)

Packet Analytics ♦ www.packetanalytics.com (2007-Present)

Granite Edge Networks ♦ *shuttered* (2006 - 2007)

Amazon.com (1999-2006)

Amazon.com ♦ Sr. Manager, Information Security (2003-2006)

Leader of the team charged with complete responsibility for defining and driving information security diligence throughout the company.

Domains of responsibility encompassed all things electronic: customer data (including that subject to compliance standards and international privacy laws); business data; financial data; merchant partner data (including AOL, Target, Toys-R-U-s); HR data (including that subject to HIPAA).

Presented periodic security briefings to the company's executive audit committee (which included members of the board of directors), to the company's primary risk insurers, and to other external entities as required by the business.

Defined security requirements for all human and machine touch points pertaining to highly sensitive customer information such as payment instruments, bank account numbers, taxpayer ids, credit scores.

Defined and enforced all enterprise security policies. Initiated a top-to-bottom policy overhaul, resulting in a comprehensive framework tuned to exemplary standards. Weighed and ruled on all requests for policy exemption.

Managed response efforts for high-severity security incidents. Initiated creation of Security Incident Response Plan.

Drove continual and systematic improvements in system, network and application security. Identified and initiated operational improvements which simultaneously improved security.

Performed technological due diligence for strategic acquisitions (including Alexa Internet, BookSurge, CustomFlix, and MobiPocket) and spinoffs (A9 and at least a dozen others, not all publicized).

Instituted policies and means to constrain the duties and visibility horizon of more than a thousand overseas contractors.

Facilitated internal security audits and managed engagements with independent world-class auditors and penetration testers. Assigned and tracked action items for each finding.

Performed business-owner diligence for significant portions of Sarbanes-Oxley Section 404, Visa CISP and PCI/DSS.

Instituted compulsory requirements for managing enterprise-wide logical access rights and privileges. Expended notable team resources to develop facilitative tools for managing the massive cartesian product of servers, server classes, people, roles and rights.

Participated on the core defense team for six highly publicized lawsuits alleging patent infringement, some with tens of millions of dollars at stake.

Represented the company at meetings of the Pacific Northwest CISO Forum (PACCISO). Other companies represented included Microsoft, Nike, Washington Mutual, Starbucks, Nordstroms, Port of Seattle, Expedia, Alaska Airlines.

Co-authored the company's open source software policies. Lobbied senior executives to liberalize portions of the policy that had previously precluded staff from publicly participating in open source projects.

Amazon.com ♦ Sr. Manager, Amazon.com Associates Program (2001-2003)

Managed the technology team that powers Amazon.com Associates, the Internet's largest affiliate network of 1M+ registered website owners.

Drove significant operational improvements of a proprietary platform that renders billions of dynamic ad impressions annually. Instituted fine-grained performance monitoring in support of SLAs. Managed the implementation and

deployment of numerous revenue-generating features including Remote Buy Box, Quick Click Buying™, and Tiered Compensation.

Drove wholesale redesign of the Associates Central extranet used by associates. This effort reduced six distinct extranets -- each with dedicated hardware, software, content, and configuration -- down to a single multi-lingual extranet now used by associates in all geographies.

Stabilized the production launch of Amazon.com Web Services Version 1.0 by writing its operations and scaling plans. Architected the throttling mechanism which defends the service against abusers.

Amazon.com ♦ Sr. Manager, Information Technology (1999-2001)

This actually represents several roles in rapid succession. Responsible, at peak, for an umbrella organization of fifty engineers on five teams.

Hallmark accomplishments included construction of the automation framework which came to enable years of massive (nearly 50X) infrastructure scaling, and enabled 2001's wholesale migration from vendor UNIX to Linux. The migration yielded a first-year savings of \$17MM (25% of technology expense), truly legitimizing Linux as a viable platform for Fortune 500 companies.

Managed ISV relationships and negotiated licenses worth street values of figures.

Verio Inc. ♦ Director, Security Engineering (1997-1998)

Groomed by the senior vice president of engineering for a significant leadership role in this Tier One ISP newly built through acquisition. At this time security services remained a noteworthy market differentiator for ISPs.

Wrote the business plan, architected and began construction of a national-scale managed firewall service based upon technology developed at NorthWestNet. After my departure to Amazon.com, this service died on the vine lacking a capable technology leader.

NorthWestNet ♦ Manager, Security Engineering (1996-1997)

This originally not-for-profit ISP was one of just ten funded by NSFNET to form the Internet's first national backbone. The company also installed the very first Internet connections for dozens of brand-recognized companies including Microsoft, Boeing, Vulcan Ventures, and Nike.

Hired after an extensive national search to incept a suite of security service offerings with three primary objectives: to serve as a differentiator for bandwidth customers; to establish new revenue streams; and to boost the company's value for acquisition. These objectives were achieved.

The task entailed building everything from the ground up: designing service offerings; hiring a team; establishing reseller agreements; forging alliances with key partners, including with Carnegie Mellon University CERT/CC; developing contractual agreements; writing software; producing market collateral; deploying infrastructure; facilitating the sales process in every way imaginable; and ultimately provisioning and serving customers. Customers spanned the gamut of industries: Internet commerce; brick-and-mortar retail; technology; insurance; health care; manufacturing; municipalities; higher education; professional sports.

The managed firewall service predated and outclassed that of many competitors. It also inspired a new product line for a publicly-traded firewall company.

Indiana University ♦ Principal Software Engineer (1986-1996)

Commenced in the department of academic computing within days of the university's first dedicated Internet circuit. Inside two years the technology-progressive university was among the first in the world to offer blanket Internet access to all of its 100,000 constituents.

Progressed from entry-level programmer to principal software engineer. Became the first staff member in university history, including the then-30-year old department of academic computing, to attain software engineer status.

Authored of hundreds of applications totaling more than a half million lines of code, some used by virtually all constituents. Acquired and applied advanced expertise in operating systems (VAX/VMS, SunOS, Solaris, Ultrix, OSF/1, IRIX, HPUX); TCP/IP networking; client/server paradigms; presentation layer protocols. Co-wrote popular open-source software for VMS, some later dual-licensed to DEC and several ISVs.

Materialized an immediate \$750,000 savings with one solo project lasting four weeks. By co-authoring the first usable POP3 email server for VMS, launched an historic shift at the university from centralized to distributed computing.

Became de facto expert for black hat intrusions, inspiring a popular book on Internet Security (*see Publications*). Trained at MIT for a successful large-scale deployment of Kerberos.

These and other accomplishments lent steady public esteem to the university's technical prowess. That later influenced the university's election to host the Internet2 NOC, a.k.a. Abilene.

Bodhi Software ♦ Founder and Principal (1988-1996)

Founded and managed this part-time consulting practice of six technology experts at peak. Clients included two Fortune 500 companies, public and private universities, and a world-renowned research lab.

Under auspices of several NASA SBIR grants held by Dr. Jeffrey Alberts, developed innovative software to help improve scientific understanding of the behavioral effects of space flight on mammals. This included one embedded system, developed entirely from the ground up, slated for a pending space shuttle mission. Although flight-ready, it never flew due to cascading setbacks from the Challenger incident.

Nuclear Measurements Corporation ♦ Software Engineer (1984-1986)

Designed and developed critical software components of radiation monitoring systems. The company's customers included nuclear power plants, radioactive waste storage facilities, and defense-funded laboratories.

Acquired extensive knowledge of real-time computing, assembly languages, device drivers and OS internals. Designed and implemented a proprietary LAN protocol for multi-node installations. Devised means of patching self-written interrupt handlers into MS-DOS.

Eli Lilly & Company ♦ Systems Analyst (1983)

Mainframe programmer for an application suite serving an international team of product flow analysts. Maintained a quarter of a million lines of COBOL and JCL.

Publications

Author ♦ *Actually Useful Internet Security Techniques*

New Riders Publishing Publishing, 1995

A pioneering and acclaimed book about Internet Security. Technical reviewers included Bruce Schneier (founder of Counterpane Internet Security Inc.), Phil Zimmermann (founder of PGP Inc.), and Christopher Klaus (founder of Internet Security Systems Inc.). Published in five languages. Remained SANS Institute Recommended Reading through 2003, five years after going out of print.

Technical Reviewer ♦ *RFC 3013: Recommended Internet Service Provider Security Services and Procedures*

The Internet Society, 2000

Technical Reviewer ♦ *Handbook for Computer Security Incident Response Teams, First Edition*

Carnegie Mellon University CERT/CC, 1998

Technical Reviewer ♦ *Designing Network Security*

First Edition, Cisco Press, 1999

Contributing Author ♦ *Implementing Internet Security*

New Riders Publishing, 1996

Contributing Author ♦ *The Webmaster's Professional Reference*

New Riders Publishing, 1996

Technical Editor ♦ *The CGI Book*

New Riders Publishing, 1996

Public Speaking

PCI-DSS Audit Preparation ♦ IT Compliance Institute ♦ November 2007, San Diego CA

Enterprise Security & Privacy at Scale ♦ IT Compliance Institute ♦ November 2007, San Diego CA

Executive Panel ♦ ISSA CISO Executive Forum ♦ March 2007, Las Vegas NV

Information Security Must Die ♦ SecureWorld Expo ♦ October 2006, Seattle WA

Service Oriented Architectures ♦ Discussion panel sponsored by Forum Systems ♦ May 2006, Los Angeles CA

XML Security: Duct Tape of the Semantic Web ♦ ISSA ♦ May 2006, Cleveland OH

Dozens more prior to 2006...

Current Memberships

Anti-Phishing Working Group ♦ Global pan-industrial and law enforcement association

Infosec Entrepreneurs Network ♦ Founder of this online group

WSA ♦ Washington Technology Trade Association

PACCISO ♦ Pacific Northwest CISO Forum

Agora ♦ Pacific Northwest security professionals

Continuing Education

Intentional Leadership ♦ Interactive computer-based course by Business Acumen Inc.

Time Management ♦ Seminar by FranklinCovey

Incident Response Procedures ♦ Trained directly by CERT/CC staff

Enterprise Scale Kerberos ♦ Trained directly by MIT Project Athena staff for an implementation of 100,000 users

INTEROP Tutorials ♦ Approximately eight, taught directly by renowned experts (e.g., Jeffrey Case, Marshall Rose)

Academic Awards

National Dean's List ♦ National Outstanding College Students (1983)

Sigma Zeta ♦ National Science and Mathematics Honor Society (1982)

Phi Eta Sigma ♦ National Freshman Honor Society (1980)

Education

Graduate Studies ♦ Mathematics

Indiana University (1986, not degreed)

Bachelor of Science *summa cum laude* ♦ Computer Science & Mathematics

Ball State University (1983)