Joshua David Knight

Joshua.David.Knight@gmail.com
LinkedIn: Joshua David Knight

LEADERSHIP & EXPERTISE SUMMARY

Serving in varying capacities over my cybersecurity career, from security engineer and architect to senior security executive (up to $203M budgets and 2320 employees), I have amassed 25 years of Security experience across corporate security (1999-2013) and client-facing engagements (2013-2024), including Commercial, Government Solutions (Defense & Intelligence) and Critical Infrastructure. I bring deep domain expertise in cyber security (advisory and infrastructure), security operations, governance risk and compliance (GRC), identity and access management (IAM), and next-generation services including Internet of things (IoT), mobile, cloud, and artificial intelligence (AI).

PROFESSIONAL EXPERIENCE

Senior Executive Security Leader
Governance, Risk, & Compliance (GRC) • Security Operations • Security Strategy

Executive Vice President, Cybersecurity and Risk Management 2019 to 2023
DIGITAL14/ADQ ▪ Abu Dhabi, UAE

Serving as Executive Vice President (EVP) over the Cybersecurity and Risk Management practice where I have 356 employees and own P&L for a $185M organization - charter is to establish a global practice as a separate operating company focused on organizations across EMEA, APAC, and the Americas countries included United States, UK, France, Germany, Australia, KSA, China, and Singapore.

- Responsible for providing Advisory (vCISO, Strategy, GRC), Architecture and Engineering, NPKI, Labs (Signal, Encryption, Hardware, Software, APP), Digital Education (LMS & HITB), Government Solutions (Defense & Intelligence), Client and Security Operations services – own operations (business services), emerging technology development, and commercial GTM.
- Led organization in building and implementing $1.8B Cyber Transformation program over 10 years – migrating all Critical Infrastructure (86 organizations) across governance and technology
- Led design of consolidated IA UAE national security controls infrastructure that includes a combination of SOC 1 and 2, HIPAA, GDPR, SOX, and others): Utilize 172 controls and services across core solutions, frameworks, security operations, human capital, and managed cyber support - domains include end-user, infrastructure applications/data, and disaster recovery/business continuity.
- Utilize mandate to design and build new technical advancements for large-scale automated security service, including $80M investment in Continues Assessment and Improvement platforms, Mobile Virtual Network Operator Security Platform (MVNOSP), Cloud Marketplace, Centralized Security Operations Center (CSOC) and Cyber Command Center
- Established phased Target Operating Model (TOM) for focused execution of 2021/2022 goals – included operating targets, processes, and KPI management.
- Implemented revised organization model by implanting off-shore/near-shore model, right sizing pyramid and workforce optimized to top billable talent (increased revenue per head from $1.1M to $1.4M), realigned executive staff cost from 22% down to 14% (saved $7.6M).
- Executed 3-year GTM strategy and commercial model across Sales, Marketing, Demand Gen, and Platforms & Services – initiated run rate business and tactical execution (SPIFF, Sales Toolkits, Solution Architects.
- Increased revenue growth from 3.27% to 12.2% in 2020, 13.4% in 2021, and 18.6% in 2022 by consolidating business units, increasing critical infrastructure market penetration, redesigning business development, and expanding global portfolio
- Defined and owned Cyber Information Security and Risk Office (CISRO) responsible for governance, technology, and physical security and risk oversight across ADQ $100B portfolio of companies:
    - Leadership responsibility for 43 companies inside critical infrastructure portfolio (Energy, Transport, Commerce, Healthcare, Media, Communications, Logistics, etc.)
    - Built a Centralized Security Operations Center (CSOC) to reduce spend from $98M to $46M using consolidated technology and staffing capabilities.

Vice President, Cybersecurity Go-to-Market 2018 to 2019

DIMENSION DATA/NTT ▪ Dallas, Texas

Serving as Vice President over the Cybersecurity Go-to-Market organization with a cross-matrix responsibility (76 employees, $203M P&L) for sales, product development, and delivery.

- Ensured industry alignment by launching 3 year roadmaps across Cyber Security, Governance Risk and Compliance, Identity Access Management, and Next Generation Services
- Actively innovated and made substantial contributions to intellectual property portfolios that helped establish new security services by generating new sources of revenue
- Worked directly with senior management across various marketing and product development organizations where we were responsible for analyzing client business processes to understand goals and strategies, and to utilize proven methodologies and tools to recommend changes that will improve the overall experience
- Used consulting services as a penetration point to shorten sales cycle and grow new deals. Smaller engagements established immediate revenue and opened us to developing long-term client partnerships that supported larger complex deals (Land and Expand) – established $14.4M in new advisory and professional services revenue
- Established centralized IT and OT policy, standards, and procedures, deep dive assessments, incident response and transformation programs.

Vice President, Cognizant Cybersecurity and Risk Management 2016 to 2018

COGNIZANT TECHNOLOGIES SOLUTIONS ▪ Dallas, Texas

Serving as Vice President over Cognizant Cybersecurity and Risk Management where I have 2320 employees and $135M budget – global responsibilities across United States, Canada, United Kingdom, France, Germany, Belgium, Luxenberg, Netherlands, Norway, India, Australia, Japan, South Africa, Brazil, and Singapore.

- Responsible for providing advisory, engineering, professional, and operations security services across Cyber Security (Network & Applications), IAM, GRC, and Next Gen (Cloud, Mobile, Analytics)
- Defined and owned all policy, standards, and procedures, security assessments, incident response and transformation programs across Cognizant inside the United States and Europe (Germany, France, UK, Netherlands, Luxenberg, Belgium, Norway)
- Effectively structured Strategy, Technology, and Alliances (STA) into a cohesive organization focused on using innovation, architecture, and partnerships to deliver leading edge technical solution
- Defined a global training program utilizing virtual university and small, trainer-led groups with a mix of presentations, exercises, role-playing and experience sharing. The objective is to define a next-generation workforce emphasizing education, emerging technology, and experiential learning

Associate Partner, Cybersecurity Advisory Services 2013 to 2016

IBM ▪ Dallas, Texas

Leader with responsibility for $13M of IBM's Professional Security Services business with 22 employees – provided advisory and professional services across 1) Security Strategy, Design, and Architecture; 2) IT Security Assessment; 3) Risk Management; 4) CISO services 5) Program Management

- Maintain P&L responsibility for organization and lead all aspects of its strategic vision, business development, partnerships, and relationships with senior executives, customers, and standards organizations in order to deliver above target profit and revenue
- Built pipeline and drove revenue using partnerships, social selling, published articles, a multipronged lead generation campaign that included events/seminars/conferences, and a substantial digital marketing investment across email/e-nurture, blogs, and webcast – CQGR growth rate of 22.7% quarterly
- Responsible for producing products and services that protect the enterprise and consumer mobile, cloud, and analytics experience while serving as the subject matter expert across key security technology areas
- Defined IoT for Cloud Service Provider (CSP) - IoT deployments through as a service model • OEMs - Device manufacturer operate & manage the infrastructure

Associate Director, Digital Security Services 2012 to 2013

ERNST & YOUNG ▪ Dallas, Texas

Associate Director inside Ernst & Young's Digital Security business (i.e. mobile enterprise, IoT, cloud computing, and data analytics) – assisted in driving P&L by delivering above target profit and revenue.

- Drove practice revenue and profit targets by building credibility, and developing and leveraging a position as a "Trusted Advisor" to key Fortune 500 clients.
- Defined current state and future state architectures across endpoint, transport, and networks by providing expert-level business and technical experience, and possessing a deep understanding of developing long-term strategies, plans, and architectures
- Informed and communicated key technology trends to senior leaders for possible new services, including the generation of solution options and alternatives, and documentation of associated decision criteria
- Contributed to E&Y's revenue and market share by establishing a new pipeline that achieved key practice signings targets, while delivering transformational engagements above target profit and revenue yield

Senior Security Architect and Lead Member of Technical Staff (LMTS), Mobility 2006 to 2013

AT&T INC ▪ Atlanta, Georgia

Served as Senior Security Architect and Lead Member of Technical Staff (LMTS) responsible for AT&T's Mobility governance and technology oversight- including network, systems, and handsets.

- Patented the Smart Mobile Computing for IoT architecture and capabilities framework as a multi-layered approach to significantly reduce costs, and improve growth and productivity, by allowing *any trusted device, anytime, anywhere in the world, over any connectivity,* while continuing to ensure protection of intellectual property and data privacy, without sacrificing compliance with security policies and government regulations
- Defined current state and future state architectures across endpoint, transport, and networks by providing expert level business and technical experience, and possessing a deep understanding of developing long-term strategies, plans, and architectures.
- Led wireless applied research in the area of handset security research activities with key industry partners (e.g. Apple, Microsoft, Samsung, Motorola, RIM, etc.) and network security research activities with key industry partners (e.g. Juniper, Cisco, HP, etc.)
- Integrated and leveraged extensive knowledge of the mobile security industry practices, methods, and procedures to generate innovative security solutions that created market opportunities through the invention of leading-edge technologies with significant value. New technical advancements for large-scale mobile security projects:
    - Authentication for Everyone (AFE): mobile security service offered as a device based biometric/token access control mechanism that utilizes a network based authentication framework
    - Virtual Private Gateway (VPG): mobile security service offered as a layer 3 SSL technology to encrypt and force all IP traffic (RF & WiFi) into a centralized network based policy control center in order to perform policy based routing in the carrier and enterprise networks
    - Secure Application Experience (SAE): mobile security service offer as a cloud based solution that integrates authentication, encrypted storage, and encrypted transport directly into the Enterprise and Consumer apps built for Smartphone's. Technology improves the user's experience by accelerating all data 3x-5x and providing an additional %15-%30 battery life
    - Endpoint Device Management: mobile security service offer that utilizes device based policy control mechanisms to protect content stored on the device. Service utilizes the following technologies
- Drove collaboration between Intel, AT&T and McAfee (led to Intel's eventual acquisition of McAfee in 2011) to further expanded the Smart Mobile Computing for IoT architecture by embedding security into Intel server, desktop, and mobile chipsets - designed to protect the AT&T core network from DDoS without having to rely on the user to provide endpoint protection

Senior Security Engineer, Corporate Security 1999 to 2006

SPRINT CORPORATION ▪ Overland Park, Kansas

Responsibilities include privacy, infrastructure, and security related activities - Vulnerability Management, Risk Management, Engineering, Network and Security Operations, Compliance, Security Awareness, SDLC, Monitoring, and Incident Response.

- Led network, hardware, and software vulnerability testing, including ethical hacking, penetration testing, and reverse engineering across internal clients technical security evaluations
- Developed and implemented risk based remediation program to address security gaps – worked with Lines of Business (LOBs) to determine risk acceptable solutions to meet security policies and solutions
- Assisted in the construction of multiple security teams from planning to completion – Compliance and Risk Management, Incident Response, Vulnerability Assessment, Privacy, Risk Management, Compliance (PCI & SOX), Security Metrics and Awareness Log Correlation and Security Monitoring.
- Embed security in key business processes; SDLC, contract negotiations; vendor contracts; new third-party relationships; new technology infrastructure; BCP/DR; strategic planning.
- Deployed Disaster Recovery/Business Continuity program (BCP/DR) and Data Leakage Protection
- Principally involved in the designing and implementing of business continuity plans.
- Experienced in e-discovery and conducting forensic computer investigations to identify, preserve, recover, analyze, and present facts in common language for evidence.
- Oversaw the creation of a daily service review for operations that incorporated all business units and stakeholders. Created the Root Cause Analysis team and the underlying processes.
- Responsible for building the ISS security center infrastructure - Vulnerability management consisted of the security center server and 37 remote scanners.
- Implemented privacy scans to locate PII throughout the enterprise.
- Established a best practice vulnerability management and hardening program.
- Devised methods of double checking security tools against security tool for audit validation.
- Took the initiative to re-evaluate and improve the security infrastructure at General Dynamics; paying special attention to internal controls, auditing, IDS, firewalls, VPNs, incident response, patch management, and documentation.

EDUCATION

M.B.A., Information Technology, 2001
Friends University ▪ Kansas City, Kansas
GPA 3.91 out of 4.0 - Presidential Honors

B.S., Pre-Medicine/Pre-Medical Studies, 1999
Friends University ▪ Wichita, Kansas
GPA 3.68 out of 4.0 - Presidential Honors