John Seitzinger, Technical Manager/Principal Consultant, Cybersecurity, Risk Management, Security Architectural, and GRC Specialist

Was Technical Manager, Optiv (12 years), now Principal Consultant, Governance – GuidePoint Security

CISSP, CISM, CISA, BCMM-A, BSI ISO 22301-LA, Enterprise Governance, Risk & Compliance

Summary

With over thirty years of professional experience in technology, and more than 26 years in cybersecurity-focused services, John Seitzinger has consulted with subject matter experts and executive management regarding technology, security, and compliance initiatives, and successfully managed diverse teams to meet business goals in global/Fortune 500 companies, small and medium businesses, and government.

Mr. Seitzinger has performed training, conducted, and overseen enterprise risk assessments, technological countermeasures / gap analysis, maturity assessments, risk assessments, security and compliance initiatives aligned to frameworks such as: NIST CSF, NIST SP 800-53r4/5, GDPR, CCPA, GLBA, HIPAA, FFIEC, ISO/IEC 27001/27002, TISAX, ISO/SAE DIS 21434 Road vehicle – Cybersecurity engineering, ISO 22301 Business Continuity Management System, and others; written prescriptive policies and standards, recommended/outlined defensive strategies and tactics, developed information security programs, integrated complex cybersecurity solutions, performed Business Impact Analysis, developed Business Continuity Plans, and project managed large scale security technology implementations as well as designed secured ecommerce architecture upgrades. Mr. Seitzinger has managed security and compliance related projects from pre-scoping / requirements gathering through proposal development and successful implementation. Moreover, Mr. Seitzinger has led diverse teams of consultants, contractors, and employees in compliance and remediation projects, specialized and consulted on global privacy regulations and transborder data flows, and developed a wide array of cybersecurity documentation, incident response plans, security dataflow diagrams and led exercises for global organizations.

Project Experience Highlights

Authored Specialized Standards and Assisted with Implementation for TISAX (Trusted Information Security Assessment Exchange) and ISO/SAE DIS 21434 Road vehicles – Cybersecurity engineering, for Leading Audio Electronics Manufacturer's Automotive Division

- Assisted company-wide cybersecurity group in authoring specialized standards to achieve TISAX certification
- Worked (work-in-progress) directly with Automotive Systems Division in operationalization efforts for ISO/SAE DIS 21434 Road vehicle – Cybersecurity engineering

Lead Technical Manager for Global Chemical Company Ransomware BIA, BCP and Contingency Plans

- Implementing highly complex ransomware Business Impact Analysis, Business Continuity Plan and Ransomware Contingency Plans (work-in-progress)

- Developed engagement tactics, project flow dynamics, and leading oversight, and Manager II Business Continuity Management System specialists to drive project

Develop Business Continuity Service Offerings for Go-to-Market for Optiv

- Own, create and establish go-to-market strategy, Statements of Work (SOWs), marketing materials, deliverable templates for multiple Business Continuity service offerings.
- Oversee and vet Level of Effort (LOE) for Business Continuity/Disaster Recovery services prior to client submission.

Policy and Standards Creation Project for Fortune 50 Global Healthcare Provider (59 documents)

- Performed large scale cross-departmental NIST CSF/NIST SP 800-53r4 Policy and Standards portfolio for a leading global healthcare provider; including policy – standards maps to facilitate maintenance, and tables with control numbers and hyperlinks to reduce compliance burden

Business Continuity Maturity Model ("BCMM") and Business Impact Analysis ("BIA") for a global Manufacturing Firm

- Performed an in-depth BCMM analysis of the organization and reported on the maturity of the existing business continuity management ("BCM") program resulting in a detailed and scored heat map of program health with a series of strategic and tactical recommendations
- The above BCMM assessment resulted in a large scale BIA and Application Impact Analysis ("AIA") covering 55 locations worldwide

In-depth Assessment of a Large Financial Services Company in response to an FTC Court Order

- Under mandate of a client Federal Trade Commission court order, performed an in-depth audit-level assessment of the efficacy of the technological security controls portfolio of a major financial firm employing the Shared Assessment Agreed Upon Procedures
- Analyzed and reported on the completeness and conformity of the top down information privacy and protection program of the same, using the Standard Information Gathering tool

Multi-Regulatory Compliance Program Development for a Fortune 100 Company

- Normalized multiple regulatory compliance requirements and performed large scale gap analysis across several regulatory frameworks
- Lead team of internal compliance personnel to identify and prioritize non-compliant controls and initiate remediation strategies
- Initiated and project managed strategic initiatives to achieve balanced compliance objectives with appropriate levels of senior leadership risk acceptance
- Developed and updated documentation of governance to support ongoing compliance requirements driven by continuous improvement processes

ISO 27001 ISMS Security Program Development for Global Company

- Developed information security policies, procedures, standards and guidelines
- Using facilitated work sessions with leadership from Information Technology, Legal, Human Resources, and European workers-council members, drove acceptance across 13 countries in EMEA and 5 countries in South America
- Assisted in the related strategic initiatives to drive remediation and achieve compliance

Business Continuity Plan Development for a Utilities Company

- Leveraged facilitated workshops with business function stakeholders to collect a detailed understanding of business processes and dependencies
- Performed a risk analysis to create detailed a Business Impact Analysis (BIA)
- Utilizing the BIA, developed the organization's Business Continuity Plan

Information Security Program Development for a Fortune 100 Global Company

- Long term information security program development project for a global ecommerce company, with 20B in revenue and ecommerce 40,000 customers worldwide
- Working directly with executive leadership, performed a large scale risk assessment to identify key control gaps
- Project managed the implementation of the company's entire portfolio of technological security safeguards
- Developed procedures, including daily security task sign-offs, to ensure a highly effective, sustainable and defendable security program existed
- Instituted and project managed the implementation of a technology based exception handling and tracking system for non-compliant processes and technologies to manage risk acceptance and drive continuous improvement

Project Management and Implementation of a Large Scale IDS System for a Big Four Firm

- Led diverse teams in long term project driving the implementation of a large scale network-based intrusion detection/prevention system monitoring traffic for 165 countries worldwide
- Drove selection and implementation of Security Information and Event Management ("SIEM") system capable of handling more than 30,000 events per second in an 11,500 node data center
- Developed governance standards for newly implemented solution and supporting resource functions
- Interviewed and trained new personnel to staff operations

Security Architecture Upgrade and Supporting Documentation for Global Steel Company

- Directed and led upgrade of security systems architectures for a Fortune 500 Company with 120 locations in North America
- Identified key security technologies supporting best practices and quality of service requirements for newly implemented SAP solution
- Developed highly detailed network diagrams for proposed and implemented security architectures
- Developed ISO/IEC 27001/27002 policy and procedure documents to support new architectures and business compliance objectives

Security Safeguard Configuration Reviews for International Financial Services Company

- Assessed technical configurations on security technologies for large financial services company
- Performed gap analysis on configuration sets and recommended configuration changes

Large Scale Vulnerability Assessment & Architecture Upgrade for International Bank

- Performed physical security assessment and testing resulting in full compromise of data center
- Performed external and internal vulnerability assessment resulting in compromise of internal firewalls and internal directory services
- Implemented design changes to security architecture resulting in enclave firewall architecture using zone-based security
- Executed hardening remediation processes on network devices and supporting systems

Security Program Management for Multiple Florida Based State Government Agencies

- Managed security programs for a number of State Government Agencies in Florida
- Designed and implemented upgrades to and new security architectures
- Developed related documentation sets and deliverables

Knowledge

- Information Risk Management
- International Data Privacy
- Security Program Design
- Risk Assessment / Compliance
- Security Architecture Design
- Business Continuity & DR
- Project Delivery Oversight
- Security Systems Implementation
- Documentation of Governance

Certifications

- CISSP
- CISM
- CISA
- BCMM® Assessor
- BSI. ISO 22301 Lead Auditor