



Josh Varela

Cyber Strategy & Technology Leader | GRC, Risk Management & Enterprise Resilience SME | CISM | BISO | CSSA | vCISO | Executive Advisor

About

Seasoned leader with over 12 years of experience developing and delivering strategic solutions for a diverse portfolio of clients, spanning start-ups to Fortune 100 companies. Proven track record in driving enterprise resilience, optimizing security strategies, aligning technology efforts with business objectives, and effectively managing and mitigating risks. Demonstrated expertise in leading distributed and cross-functional teams, advising and influencing senior leadership, and implementing sustainable solutions to enhance and mature cybersecurity efforts. Proficient in designing and executing high-impact cyber strategies, leveraging advanced technologies, and integrating industry best practices to strengthen the organization’s security posture.

Bachelor’s degrees in Information Network Technologies and Business Administration, along with various industry-recognized certifications. Bilingual proficiency in both English and Spanish.

Skills & Expertise:

Cyber Strategy, Security Strategy & Roadmap Development, Governance, Risk, and Compliance (GRC), Risk Management, Security Capabilities & Maturity Assessment, Enterprise Resilience, Ransomware Readiness, Business Impact Analysis (BIA), Business Continuity/Disaster Recovery, Cyber Recovery, Network & Security Operations, Security Program Development, Policy Development, Regulatory Compliance, Strategic Incident Management Advisory (SIMA), Business Information Security Officer (BISO), Chief Security Strategy Advisor (CSSA), vCISO, Executive Advisor

Industry Certifications

- Certified Information Security Manager (CISM)
  - Certified GRC Professional & GRC Auditor
  - Certified Agile Project Management and Delivery
  - Payment Card Industry Professional (PCIP)
  - AWS Certified Cloud Practitioner (AWS CCP)
  - GIAC Security Essentials Certification (GSEC)
- CMMC Certified Registered Practitioner
  - Certified SOC Professional (CSOC-P)
  - Certified in Cybersecurity (CC)
  - Cisco Certified Network Associate (CCNA)
  - CompTIA: A+, Network+, Security+

RECENT PROJECT EXPERIENCE (NON-EXHAUSTIVE)

CLIENT & PROJECT	ROLE	ACHIEVEMENTS
Global Tier 1 Investment Bank: MVO (Minimum Viable Operations) Global Resilience Project	Business Information Security Officer (BISO)	<ul style="list-style-type: none"><li>Developed MVO Resiliency strategy aligned to business objectives and industry best practices</li><li>Identified critical systems, processes, and dependencies for resilience focus</li><li>Conducted comprehensive risk assessments to identify vulnerabilities and potential failures</li><li>Assessed existing resilience capabilities for readiness against disruptions</li><li>Designed resilient architecture strategy for key systems and processes</li><li>Collaborated with cross-functional teams to align with project goals</li><li>Conducted rigorous testing, refining plans based on outcomes and lessons learned</li><li>Documented MVO strategies, procedures, and response plans</li><li>Provided regular reports to senior management on project progress, risks, and enhancements</li><li>Developed training programs for staff on MVO procedures during disruptions</li><li>Raised organizational awareness on resiliency and continuity planning importance</li></ul>
Fortune 100 Healthcare Services Provider: Cyber Resilience Program	Business Information Security Officer (BISO)	<ul style="list-style-type: none"><li>Led the development of a comprehensive cyber resilient program, driving the security strategy across the organization to further mature functional capabilities aligned to regulatory and compliance requirements (i.e., HIPAA/HITRUST)</li><li>Engaged with business unit leaders to better understand processes and strategize best approach to integrate into the corporate resilience program</li><li>Influenced adoption of security principles and best practices (i.e., security-first mindset model)</li></ul>
Fortune 100 FinTech Services Company: Legacy Process Transformation & GRC Modernization	Business Information Security Officer (BISO)	<ul style="list-style-type: none"><li>Led and coordinated a team of security professionals through a legacy process transformation &amp; GRC modernization initiative under office of the CISO and Chief Compliance Officer (CCO)</li><li>Conducted workshops with functional leaders to understand current processes, inventoried thorough documentation for completeness, including interdependencies observed and reported redundancy/overlap to CISO, providing insight for process uplift and modernization</li><li>Functional oversight for mapping processes to security controls and regulatory requirements with full integration and tracking within corporate GRC platform</li></ul>
Fortune 500 Industrial Services Company: Cyber Resilience Program	virtual Chief Information Security Officer (vCISO)	<ul style="list-style-type: none"><li>Closely worked with the CTO and CISO to develop and implement an Enterprise Cyber Resilience Program to better position the organization against cyber events</li><li>Reviewed and improved Corporate Governance to align with Cyber Strategy</li><li>Functional oversight for security strategy and coordinated efforts with relevant parties</li><li>Revamped the Incident Response capabilities to support an Enterprise Resilience Program</li></ul>
Large National Retail Company: Security Program	Chief Security Strategy Advisor (CSSA)	<ul style="list-style-type: none"><li>Led design, development, and implementation of a tailored, robust security program</li><li>Engaged with leaders across the business to better understand processes and strategize best approach to integrate into the corporate program</li><li>Oversaw mapping processes and security controls to regulatory requirements within the corporate GRC platform</li><li>Advised senior leadership on security priorities, incident response planning, compliance, and robust controls</li></ul>

# PROJECT EXPERIENCE (NON-EXHAUSTIVE)

CLIENT & PROJECT	ROLE	ACHIEVEMENTS
Large Multinational Retail Company: Cybersecurity Program Maturity	Chief Security Strategy Advisor (CSSA)	<ul style="list-style-type: none"><li>Under office of the CISO/CTO, collaborated with InfoSec Sr Leadership to mature corporate security posture and eliminate redundant inefficiencies where possible</li><li>Enhanced Security Awareness &amp; Training program to include role specific training modules</li><li>Oversaw segmentation, system hardening, vulnerability and patch management, and EOL remediation, among others</li></ul>
Fortune 500 Finance & Insurance Company: Ransomware Readiness Assessment	Chief Security Strategy Advisor (CSSA)	<ul style="list-style-type: none"><li>Managed engagement team responsible for delivering comprehensive solutions</li><li>Identified opportunities for improvement across people process, and technology to enhance the ability to prevent, detect, respond, and recover from ransomware threats</li><li>Developed comprehensive remediation plans to enhance the protection and rapid recovery of critical business processes and core system dependencies</li></ul>
Fortune 500 Financial Services Company: Incident Management Program Review	Sr Manager, Strategic Incident Management Advisor (SIMA)	<ul style="list-style-type: none"><li>Conducted workshops with key stakeholders to understand current Crisis &amp; Incident Management lifecycle and gather relevant documentation</li><li>Implemented and standardized a dedicated framework, aligned to the organizations needs and appetite</li><li>Developed policies, standards, and procedures to align with the newly adopted framework</li></ul>
Large National Payroll Services Provider: Cyber Recovery Capability Enhancement	Chief Security Strategy Advisor (CSSA)	<ul style="list-style-type: none"><li>Managed and led the engagement team in the development of an enhanced, corporate wide functional cyber recovery program</li><li>Coordinated workshops with key stakeholders and SMEs to gather information relevant to current practices</li><li>Ensured recommendations aligned to functional capability enhancements</li></ul>
Large Educational Services Organization: Security Strategy Assessment	Chief Security Strategy Advisor (CSSA)	<ul style="list-style-type: none"><li>Managed team conducting the Security Strategy Assessment</li><li>Conducted workshops with Sr Leadership to discuss current security initiatives, challenges, and desired target state, based on industry sector/size/risk exposure</li><li>Coordinated workshops with SMEs to collect relevant security practice details and associated documentation</li><li>Ensured roadmap alignment to goals based on maturity and desired state</li></ul>

CLIENT & PROJECT	ROLE	ACHIEVEMENTS
Regional Retail Bank: Security Maturity Assessment	Sr Manager	<ul style="list-style-type: none"><li>Led and conducted a Security Maturity Assessment based on FFIEC and NIST CSF, reporting directly to CISO and internal Audit</li><li>Met with SMEs and key stakeholders to discuss current security posture and practices</li><li>Identified weaker, less mature areas and provided recommendations aligned to industry standards and best practices</li></ul>
Large Multinational Retail Company: PCI DSS Audit	Sr Manager	<ul style="list-style-type: none"><li>Led end-to-end PCI DSS audits, coordinating with internal teams</li><li>Collaborated with diverse teams, including IT, compliance, and business units, to foster a holistic and integrated approach to PCI compliance</li><li>Conducted in-depth technical assessments of in-scope systems and networks</li><li>Maintained documentation outlining compliance strategies and procedures</li><li>Implemented continuous improvement initiatives based on audit findings</li></ul>
Large Healthcare Organization: HIPAA & Data Privacy Assessment	Sr Consulting SME	<ul style="list-style-type: none"><li>Developed and executed strategic HIPAA compliance assessment</li><li>Led end-to-end assessment, managing internal teams and collaborating with organizational stakeholders</li><li>Oversaw the implementation of robust security controls for safeguarding sensitive data (e.g., PHI, PII, etc.)</li><li>Designed and delivered targeted training programs for staff awareness</li></ul>
Multinational Stock Photography, Video, and Music Company: Business Impact Analysis	Sr Consulting SME	<ul style="list-style-type: none"><li>Led and conducted BIA, coordinating with internal teams and stakeholders</li><li>Conducted comprehensive risk analyses to identify critical business functions and dependencies</li><li>Maintained documentation outlining BIA methodologies, findings, and recommendations</li><li>Integrated BIA into developing and enhancing business continuity plans</li></ul>
National Dental Insurance Services Company: Data Privacy Assessment	Sr Consulting SME	<ul style="list-style-type: none"><li>Led a Data Privacy assessment to evaluate current practices and capabilities, managing internal teams and collaborating with organizational stakeholders</li><li>Conducted a comprehensive analysis of current controls to identified gaps and improvement opportunities</li><li>Conducted in-depth technical assessments of in-scope systems and networks</li><li>Developed comprehensive remediation plans to enhance the protection of sensitive data, processes, and core system dependencies</li></ul>