Brian W. Haugli

brian.haugli@gmail.com | 518-637-3831

Brian Haugli is a proven security leader, entrepreneur, mentor focused on building high performance teams, operating models, and delivering quality based risk management capabilities for global enterprises. Brian is instrumental in establishing well defined security strategies to align in the support of business objectives and results. He has outstanding communication skills, a positive demeanor, and the ability to interface with all levels of an organization. Brian is regularly requested and involved with speaking engagements, keynotes, panel discussions, podcasts, and interviews as a recognized expert in the industry. He serves on his alma mater, Morrisville State College's Board of Directors as well with the US Marine Corps Cyber Auxiliary.

Managing Partner & Co-Founder, SideChannel Security April 2019 – Present

Tech-enabled services company focused on cybersecurity consultancy for start-ups, small businesses, & mid-market organizations

• Established a vCISO offering tailored to mid-market companies and smaller. Service is subscription based and financially affordable for companies with under $3B in revenue.
• Directs a development team to create a SaaS platform to condense assessment process and automate data gathering for clients in order to ramp up vCISO and strategic work
• Led growth of sales volume and focus, growing sales to over $300,000 in first year of full-time operation. Closed on average 60% of leads and achieved sales goals for both services and product.
• Led growing sales to over $1.400,000 in first 6 month of 2020 and during COVID.
• Attracted and trained top tier CISOs to join services team; team member bios available on website: https://www.sidechannel.com
• Built successful marketing plan, production, and distribution channel to operate at scale with minimal overhead; YouTube, LinkedIn

Vice President & Chief Security Officer, The Hanover Insurance Group May 2015 – April 2019

Corporate Security Office across US domestic and international information and physical security operations

• Consistently rated as achieving or surpassing performance standards year over year. Management, peer and Board feedback all score high with delivering on promises, being able to quickly get at root cause, willing to invest time to learn and ability to communicate complex subjects in layman's terms.
• Developed & delivered the strategic vision, resources, and protocols to maintain enterprise IT security, mitigate risk, oversee vendor risks, and influence user behavior by elevating the profile and importance of information security at the company.
• Developed and managed a $7.5 million budget by 2019 in line with strategic growth needs supporting information security. Responsibly grown from $500,000 budget in 2015 to address key risks based on priority and impact.
• Brought together key security and risk stakeholders to design, develop, refine and review enterprise IT security and risk strategies, including, the development and maintenance of NIST standards that meet the company's needs.
• Structured, hired, and retained new team of engineers and analysts to address information security and data protection risks for company. Grew team appropriately and cost consciously over 4 years on global scale. Thoughtfully leveraged outsourced managed service solutions alongside onsite personnel to create a productive and meaningful collaborative atmosphere for team members.
• Acted as lead representative on all information and physical security initiatives for all stakeholders. Regularly interfacing with the enterprise risk management group, legal, human resources, and internal audit, in regard to company policies, procedures and plans.
• Regularly briefed the Board of Directors, Audit Committee, and corporate executive leadership of risks and plans to address.
• Acts as lead representative with internal and external auditors regarding assessments and testing of information security and risk management. Significantly decreased amount of delinquent or open audits within first 6 months in role. Continue to manage an appropriate level of audit findings and balancing costs to close versus risk mitigated.
• Exercises decision making authority on risk assessments and mitigation, overseeing process to ensure risks have been addressed, acting as policy making authority, creating roadmaps, technology priorities and solution proposals and recommendations, as well as managing department budget.
• Developed key working groups and reorganizational structures for better insight and visibility of risk for business leads and owners
• Developed and implemented new plans for security incident response. Oversaw tabletop exercises to ensure that all stakeholders were involved and knowledgeable about their responsibilities. Successfully exercised plans in both actual responses and training scenarios through red team and penetration tests. Executive leadership and Board of Director viewed all as reasonable and suitable.
• Designed, implemented and managed full stack open source threat hunting platform; Elasticsearch, Logstash, Kibana, Suricata, Snort, & Bro. Integrated with critical asset log sources and end-point detection & response capabilities; Carbon Black, Ossec, GRR
• Designed, implemented, and managed open and closed source intelligence gathering platform using STIX/TAXII, CSV, & CEF
• Implemented and managed successful user behavior analytics platform to identify user and account-based threats within the environment. Successfully detected and responded to insider threats through capture of and correlating web traffic, user habits, file access, and physical movement. Integrated metrics into human resources and legal processes to expedite issue resolution.
• Implemented and managed open and closed source vulnerability management/remediation platform; OpenVAS, Nessus, Tenable.io
• Designed and implemented open source phishing simulation platform to test end-user awareness and inform training opportunities

• Coordinated investigations and responses to all security incidents. Recommended and implemented countermeasures to reduce impacts and risks of future related events or incidents.

Information Assurance Program Management Division Lead, CGI Federal Oct 2011 – May 2015

U.S. Department of Defense, US Army ITA, Enterprise Information & Mission Assurance

• Directed a team of 35 cyber security professionals across multiple disciplines in separate geographic locations.
• Lead strategic initiatives for Pentagon on cyber security, information risk management, auditing, and compliance.
• Applied subject matter expertise and knowledge of current IA policy, tactics, techniques, policy, doctrine, and relationship to IA reporting requirements and structure. Working knowledge of NIST 800-30, 800-37, 800-39, 800-53, CSSNI 1253, & DoD instructions
• Directed and lead 4 successful Department of the Army Inspector General (DAIG) inspections & audits for customer over 3 years
• Developed methodology and reporting capability for tracking & managing exploit category vulnerabilities to increase compliance
• Designed and developed based tracking system for enterprise and system level POA&Ms for customer
• Developed methodology and reporting capability on Insider Threat for DoD based on RMF and NIST framework
• Active member of the US Army CIO working group on Risk Management Framework implementation for Army ICS systems
• Developed high quality assessments that provide an understanding and resolution to security-related events as they occur.
• Assessed impact, determined probable damage and suggested methods of damage control, conducted in-depth analysis, and follow-on investigation to build historical and predictive capabilities.
• Analyzed and recommended resolution of security problems based on expert knowledge of the major IA products and services, a vast understanding of their limitations, and a superior knowledge of the disciplines of IA.

Senior Systems Architect, RPI Oct 2010 – Oct 2011

U.S. Department of Defense, National Reconnaissance Office

• Supported critical classified operations for intelligence community customer
• Managed security requirements and solutions for customer; meeting requirements and obtained authority to operate for each system
• Directed all activities related to virtualization, storage, and security for large scale critical national security operation

Enterprise Architect, Vangent Oct 2008 – Oct 2010

U.S. Department of Defense, Military Health System, Force Health Protection and Readiness

• Directed the technical development and implementation of projects on all classification levels
• Provided architectural and technical guidance for software, systems and network security
• Assessed current infrastructure to identify key risk areas and insure adequate level of control were implemented
• Developed disaster recovery plan in compliance NIST 800-34, DoD 8580.02R, DoD 8500.2 and MHS guidelines
• Initiated, implemented, and validated systems via DoD Information Assurance Certification and Accreditation Process (DIACAP)

IT Manager, Resolvit, Vienna, VA June 2007 – Oct 2008
IT Consultant, TechAssist, LLC, Washington, DC Oct 2006 – June 2007
Network Administrator, Schott Fiber Optics, Auburn, NY Jan 2006 - Aug 2006
Network Security Analyst, Morrisville State College, Morrisville, NY Jan 2003 – May 2005
Security Engineer, SecTech Solutions, Boulder, CO July 1998 – Dec 2002

Education

Bachelor of Technology, Information Technology in Network Administration
Morrisville State College, Morrisville, NY

Certifications & Achievements

• Certified Information Systems Security Professional (**CISSP**)
• Global Industrial Cyber Security Professional (**GICSP**)
• CompTIA Security+
• Eagle Scout

Memberships

• Morrisville State College, Board of Directions, Finance Committee
• United States Marine Corps Cyber Auxiliary, Cyber Expert