Edward J. (Rodriguez) Liebig, CISSP, CISM

IT/OT Cybersecurity Executive

Growth Enablement and Critical Infrastructure Protection

St. Louis, MO
(636) 388-2625
ed@ed.liebig.com
linkedin.com/in/liebig
eliebig.com

Leadership Profile

- Driven by, and dedicated to, guiding and contributing to the overall success of an organization through comprehensive information and security strategic program depth, breadth and management.
- Demonstrative comprehensive experience in executive-level leadership of highly complex IT and security organizations, across varying risk profiles, in numerous industry verticals.
- Developed, negotiated and executed multiple multi-year/multi-million dollar service and alliance contracts from both buyer and seller perspective.
- Accomplished at establishing threat metrics and risk profiles while proficient in leading the creation of risk tolerance through the design and implementation of a fortified bastion of people, process and technology.
- Well-seasoned in identifying, researching, evaluating and proactively addressing global threats while leveraging the most relevant technological and process-related advancements.
- Frequently monitor and contribute to public and private sector information sharing consortiums such as IT-ISAC, InfraGuard, ICS-ISAC,US-CERT, ICS-CERT and Michigan Cyber Initiative.
- Contributed hours of expertise to the creation of standards for Information Technology (IT), Operational Technology (OT) and Industrial Control System (ICS) security through ICSJWG and ISA affiliations.
- Advise fellow executives and board members (both internal and for clients) around the Value Of Investment (VOI) for IT and security initiatives as well as the business risks associated with information security events.
- Extensive knowledge of the integration of Service Level agreements, security standards, security controls, risk assessments and performance metrics into overall Governance Risk and Compliance (GRC) frameworks.

Areas of Expertise

- IT / Security Budgetary Oversight
- CCPA/CPRA, GDPR, CIP, CIS, NIST, HIPAA, HiTrust, ISO and CMMC
- Framework / Regulatory Assessment & Compliance
- Transformation and Change Management
- Strategic Planning & Roadmap
- Practical Proof of Concept Testing
- IT / Cybersecurity Consulting
- Incident Response
- Technology Assessment
- IT Infrastructure Management and Development
- High-Performance Team Mentorship
- Revenue Generation
- Program / Project Management
- Contract Negotiations
- IT & Security Tool Management
    - Implementation
    - Business Rule Definition
    - Policy
    - Operational Sustainability
    - Configuration Management
    - Sample Technologies & Programs
        - DLP, SEIM, SOAR, EDR, Penetration Testing, Forensic Analysis, eDiscovery

Education

Master of Science (MS) in Information Technology, Information Assurance and Security, Capella University
Bachelor of Science (BS) in Business Management, University of Phoenix
US Navy, "A" School for Data Processing
US Navy, "Computer Repair" School
US Naval Security Force
USN Shore Patrol

Professional Experience

Yoink Industries LLC – 2020-Present
Chief Executive Officer (CEO) and Founder
Incorporated in 2019, started pursuing business after leaving my post at Charter.

- Leader of services and delivery for Cybersecurity Consulting, vCISO, Cybersecurity Certification Training, and Cyber-Range services.
- Highly experienced and internationally recognized Information Technology/Cybersecurity Leader with extensive experience in diverse industry verticals.
- Establishes Cybersecurity Programs and IT/OT Operations, utilizing threat metrics/risk profiles to strategize IT and cybersecurity solutions.
- Well-versed in defining and managing overall cybersecurity programs for large multi-national and highly regulated Critical industries such as Financial Services (Banking, Insurance, Stock Trading), Other Critical Infrastructure (Chemical, Healthcare, Electrical, Telecommunications, transportation, natural resources) and Government (federal border protection, state infrastructure, and DOD systems) From idea through comprehensive implementation, these programs mitigate cybersecurity and risk management pitfalls.
- Orchestrated the formation and hiring of high-performing teams integrate technological requirements to increase revenue and business operations.
- Skillful negotiator of multi-million-dollar contracts that boost infrastructure, organizational efficiency and eliminate downtime.
- Metrics-driven problem-solver with pinpoint accuracy.
- Serving Delviom LLC 05/2021-09/2021 as CISO then transitioned to a Virtual (vCISO) position, led the definition and build out of their Cybersecurity Consulting practice and supported as executive interface with their client engagements.
- Responsible for internal security CMMC and regulatory control assessment and associated implementations.
- Under Yoink Industries, also serve as CISO and Technology advisor Fast Data Connect (FDC), a boutique consulting & IT services firm that is helping mid-to-large sized companies solve their problems & challenges that range from people, processes, technology, cost to end-to-end transformation. The role is to be on call as the executive liaison for all matters of Cybersecurity.

Charter Communications – 2017-2020
Vice President, Information Security Operations & Security
A senior executive with oversight of IT Security Operations, Incident Response, Security Quality Assurance, IT/Security Budget ($100M) and IT Security Strategy. Successfully led the build-out of the security operations, Incident Response, Defensive Security and GRC teams while guiding key projects through to successful fruition (on budget and on time). Starting with a NIST 800-53 assessment on IT's security capabilities, I crafted a Security Roadmap to guide future progress. Cross-referencing the 800-53 examination to the NIST Framework for Critical Infrastructure, I blended the results into the overall corporate security goals. This structured approach proved instrumental in reducing the operating budget through efficiencies and automation while increasing security posture and accountability. I created and implemented a Secure Development Framework to guide Security throughout the SDLC and overall application lifecycle. I led the Charter / Spectrum Leadership team from a technological view of security to fully realize there was more business involvement necessary to fully cover the threat profiles. I also led them through and socialized, recommended regulatory compliance processes for AML,GDPR, and CMMC.
Key Results

- Created an organizational structure that matched skills and limited headcount to cover Security Operations efficiently, Incident Response, Security QA and IT Security Infrastructure project management and execution. By optimizing the team and subsequently the operational budget, I drove a savings of $30M+ by renegotiating major Security Tool contracts, reducing redundancy, boosting efficiency by capitalizing on DLP technology, SEIM tools, EDR, SOAR, and strengthening operational effectiveness.
- Transformed the organization to recognize that security is more than technology and that many aspects of business-driven security activities had not been incorporated into the overall risk measurement (defending against a growing insider threat).
- Created and implemented a "Bow Tie" threat metrics process that successfully allowed the organization to front-run potential disruptive or nefarious activity leading up to and through prominent "high profile" events like the Republican National Convention and the Democratic National Convention.
- Provided a multi-year strategic plan that not only looked at technological advancements but took into account operational sustainability, cultural impact, and maintained a satisfactory end-user experience.
- Managed allocated budget year-over-year to achieve (and in many cases, overachieve) expectations.

Key Initiatives/Activities

- Application Rationalization and normalization of dissimilar applications across the blended enterprise after MA&D activity.
- Standardization of security toolsets.
- The transition of limited appliance-based web filtering capabilities to an integrated Palo Alto firewall/AD driven, customizable web filtering schema.
- Selected and implemented DLP technology in alignment with culture, user expectations and operational sustainability.
- Researched, tested and selected data classification tool to augment and kick start the DLP program and relieve much of the end-user burden for success.
- Researched and implemented a SEIM tool to assist in the concatenation of security event alerts.
- Researched and implemented Endpoint Detection and Response (EDR) tools to reduce the endpoint resource utilization and increase efficiency/effectiveness of the discovery and sequestration of data, and aid in incident response.
- Researched and recommended SOAR tools to pull alerts and data from dissimilar network segments to gain greater enterprise visibility of risk and events.
- Orchestrated the creation of general and specific playbooks for Incident Response across all areas of IT and OT.
- Guided the culture to embrace a cross-functional IR team to address insider threats (culminating in the formation of the Internal Risk Working Group or IRWG).

Webster University – 2016-2020

Adjunct Post Graduate Level Cybersecurity Professor

Taught online classes to master's degree candidates. Area of specialty includes Introduction to Cybersecurity, Industrial Control Systems Security, and Security Organizations Management.

Unisys – 2015-2017

Vice President, Global Security Systems

I was the senior executive leading the security delivery capabilities companywide with nine directors/VP's and 130 direct reports while leveraging a virtual workforce of over 320 additional resources. Areas of responsibility included Strategic Consulting, Technical Consulting (to include penetration testing, forensic analysis, and War Gaming), Physical Security, Industrial Control System Security, Security Product Implementation and Systems integration, and Fully Managed Security Services.

Key Results

- Consolidation of security personnel from across Unisys.
- Transformed the organization to a service-centric execution model, which contributed or led to:
    - I drove the turnaround and salvage of key client "at-risk" engagements and relationships from dissatisfaction to the purchase of more services from our security team.
    - Identified and negotiated alliance partnership opportunities.

- The identification of additional sales opportunities in established client environments.
- Nurtured client relationships to establish long term partnerships and lucrative sales opportunities.
- Through my client relationship approach, I grew one client from a $2M security consulting engagement into a $44M MSSP contract that is still growing. My practice grew another client from a quick security assessment into a $10M+ security roadmap project that may culminate in an MSSP contract.
- I led the strategic direction for very high visibility projects, both commercial and the public, to high client accolades.
- Better visibility into global assets, costs, and revenue by consolidating the security teams globally.
- Aligned uniformity amongst delivery methods and sales approaches globally.
- Instrumental in establishing key alliance partnerships for specialty security capabilities.

Key Initiatives/Activities

- Cybersecurity readiness and program creation for Super Bowl 50: Worked with the City, State and local Police, Fire Departments, light rail, FBI, DHS, NFL, CBS, and surrounding community governments to establish security response and a comprehensive Concept of Operations guideline that was used up through the event and is now a standard. I received accolades from all stakeholders.
- Data Center Consolidation: Migrated 53 State data centers down to 3 while creating centralized cloud-based security capabilities leveraged across the various government agencies. (Physical move and testing of compute assets in under 60 days).
- One of the leadership team responsible for negotiating and integrating Unisys Micro-segmentation software on Azure and Amazon Web Services.
- Redesign network segmentation between IT and OT environments to safeguard critical infrastructure in two energy companies.
- Assembled, empowered and led a global team of CISO advisors that work with clients to set strategic objectives and achieve improved security program results.

CSC Inc. – 2005-2015

Managing Partner & Global Chief Technology Officer (CTO), Cybersecurity Consulting

Guided and provided Quality Assurance (QA) for the strategy, delivery, and execution of consulting services for CSC's "Global 1000" clients. I served as the alliance director for the Cybersecurity consulting team to forge business partner relationships.

Key Results 2013-2014

- Responsible for the successful delivery of consulting services across all accounts globally.
- Standardization of the methodologies and delivery capabilities across geographic regions and industry verticals.
- The initiation of 18 new strategic consulting services globally (most recently completed the creation and launch of CSC's Global Incident Response Program) which contributed or led to:
  - 31 New Global 1000 clients
  - 20 New Managed Security Service Opportunities worth multiple millions of dollars
  - 153 Consulting engagements supporting over 60 global clients
- Cybersecurity consulting offerings and initiatives span across the Financial Services, Chemical, Energy, Natural Resources, Manufacturing, Health Care, Telecommunications and Retail Industry verticals.

Cybersecurity North American Practice Director

The leader of the strategic and tactical/technical Cybersecurity teams for the Americas. Directed staff activities, hiring and retention. Instrumental in maintaining the pipeline of opportunities and closing new business. Successfully kept staffing and execution capabilities throughout the overall CSC business transformation process.

Key Results

- Fostered relationships and cross-selling opportunities between the legacy silos of sales channels.
- Made significant contributions to the "go forward" operational strategies for the emerging operating model.
- Continued to grow client relationships for follow-on and related project work.
- Further developed, defined, and packaged our Industrial Control System assessment offering.

Principal Security Architect

I consulted with hundreds of clients for strategic and tactical business and technical security initiatives. Project managed teams as large as 85 consultants on any given engagement. I developed and socialized security

methodologies and an assessment program that addresses the Chemical Facilities Anti-Terrorist Standards (CFATS) Regulatory requirements for the Chemical Sector (which has become a standard offering).

Key Results

- Directed the development of CSC's Enterprise Security Roadmap (ESR) methodology.
- Empowered client organizations to avoid, minimize or transfer the risk and impact of security challenges. Successfully performed security program assessments, threat analysis, risk assessments and remediation roadmaps for over a hundred chemical facilities across the globe.
- The ESR and ICS assessment methodologies have become the basis for CSC's Smart Grid, Smart Mine, ICS and Information Security Road-mapping and assessment processes.
- Instrumental in obtaining follow-on and related project work with the majority of engagements. Received only positive feedback on all project work with clients.

Omgeo LLC – Boston, MA – 2006-2007

Chief Information Security Officer

While on hiatus from CSC/Travel - Defined and identified, in a "greenfield" environment, cross-functional security teams to monitor security controls, analyze trends, identify and mitigate threats, and provided proactive instruction to networking and support personnel. Led the security operations of network engineering, application development, computer and business operations toward compliance with government regulations and industry-accepted practices. Directed network security monitoring, intrusion detection/prevention and vulnerabilities assessment tools/deployment.

Established a highly acclaimed vision and three-year improvement plan to address identified U.S. Securities and Exchange Commission (SEC) audit deficiencies and additional enhancements to ensure the business-critical technologies' availability and recovery.

Developed, implemented, and monitored a strategic, comprehensive enterprise IT/OT cybersecurity program. Drove security standards across the organization, including information security policies and guidelines
Data privacy; Data classification; Endpoint security (EDR); Training (end-user and IT/OT/Security Staff) and, Testing (Tech POC, AppDevSec, etc.)

Established and maintained Threat Hunting, Threat assessment/prioritization, and Threat Profiling Security Operations (SOC Ops) to monitor the external environment for emerging threats and proactively consult with stakeholders on appropriate courses of action. Established Cross-Department/Division Incident Response process to recover and protect the business/brand from events. Engaged senior leadership across the organization to communicate the cybersecurity strategy and key information security initiatives.

Key Results

- Gave the organization a previously deficient resilience to thwart attacks on network/information technology assets.
- Successfully convinced the SEC to eliminate all significant findings from their (3) failed audits based on my vision/roadmap.

Manulife Financial – Boston, MA – 2001-2005

Chief Information Security Officer (AVP, Global Information Systems Security)

Successfully realigned IT practices to effectively safeguard information assets; restructured and improved all major IS functions for overall security and efficiency. Established and directed security and operations of network engineering, telecommunications, application development, computer, and business operations. Collaboratively authored, socialized, and implemented Global Security policies and standards. Developed and rolled out comprehensive Network and Application Development Architecture Guidelines. Designed, justified, and established an organization-wide risk management initiative.

Key Results

- Aligned and established security governance for global business units across 52 countries.
- Designed, justified, implemented and improved a decentralized security governance program.
- Empowered business units to meet business objectives while maintaining security and compliance.
- Served as a member of the executive management committee on special studies and new product selections.

Ajilon LLC – Reston, VA – 1996-2001
Project Manager / Director / Staff Manager
As an integral part of the development of Ajilon's Information Security practice, I provided IT Management Consulting with a focus on security, networking, and business continuity planning. Member of the Managed Services Security team based out of Mechanicsburg, PA, deployed nationwide out of St. Louis, MO.
Key Results

- Managed 10 direct reports (billable consultants) to guide customers through the implementation and deployment of IT, Security, and Business Continuity Planning initiatives. Delivered projects accurately, on time and according to budget.
- Congruently, I managed client engagement, including System Transformation, Extranet, Internet Application Development, Business Continuity Planning, Web Application Design Security and LAN/WAN Expansion.

I supplied our clients with Corporate-wide risk analysis, while engaging Cybersecurity with business management and other stakeholders. The program included:

- Security Threat Profiling
- I was the Creator of "Threat Bow Tie" assessment process
- Threat Assessment and control gap analysis
- Emerging Cyber and business threat analysis
- Continuous review and re-engineering of security controls and processes to efficiently reduce and manage risk Compensating and Mitigating Control enhancement recommendation
- Data Protection, Data Loss Prevention and Encryption technology selection and implementation
- Security control processes to integrate into the SWIFT, Fed-Wire, and CHIPS system
- Identity & Access Management and Privileged User Access strategy, technology and implementation
- Practical Proof of Concept Testing
- General IT / Cybersecurity Consulting
- Third-Party Information Security Assessment Program management
- Secure Development Lifecycle (SDLC) policy, process, and testing definition, and management.

Certifications / Awards / Community Service / Clearance

Certifications

- **CISSP** Cert # 25400 (Certified Information Systems Security Professional), Member of ISC2
- **CISM** Cert # 309433 (Certified Information Security Management), Member of ISACA
- **CCISO** (Certified Chief Information Security Officer), Member of EC-Council (Lapsed - re-certifying 2Q-2022)

Awards

- Awarded Sailor of the Year 1992 for Pacific Operations Support Facility
- Nominated for the Sailor of the Year 1992 for the Pacific Fleet
- Recipient of three Navy Achievement Medals and a letter of commendation from the CINCPACFLT

Community Service

- Annual March of Dimes volunteer
- Ancient Free & Accepted Mason (A.F. & A.M.) Grand Lodge, MA
- Moolah Shriner Supporting the Shriner's Hospital for Children
- National Brittany Adoption Network and New England Brittany Rescue – Volunteer
- Patriot Guard Riders supporting fallen warriors and their families

Clearance

- *TS/BI* while serving in the US Navy
- Most recently, *Secret* Clearance with the DHS through working with the DHS and TSA