Edward J. Liebig
IT/OT Cybersecurity Executive | Growth Enablement
St. Louis, MO | (636) 388-2625 | Liebig@wustl.edu | linkedin.com/in/liebig | eliebig.com

LEADERSHIP PROFILE

Edward J. Liebig is an internationally recognized Information Technology and Cybersecurity Leader with 42 years in IT and 32 years securing critical systems worldwide. He delivers Cybersecurity Programs and IT/OT Operations, leveraging threat metrics and risk profiles with deep expertise in 800-53, ISO 2700x, ISA/IEC 62443 and NIST 800-82r3, 800-171r3 to craft tailored solutions for industrial control systems and critical infrastructure. Skilled in leading comprehensive cybersecurity initiatives—from vision to execution—for multi-national, highly regulated sectors including Financial Services (Banking, Insurance, Stock Trading), Critical Infrastructure (Chemical, Healthcare, Electrical, Telecommunications, Transportation, Natural Resources), and Government (Federal Border Protection, State Infrastructure, DOD Systems), he enhances security and resilience through advanced threat assessment and control gap analysis aligned with industry standards. A metrics-driven problem-solver, Edward negotiates multi-million-dollar contracts that optimize infrastructure, eliminate downtime, and drive revenue, pioneering innovative tools like the "Threat Bow Tie" process to strengthen OT security. His dynamic leadership blends strategic vision with a rare ability to communicate complex concepts to boards and technical teams alike, fostering high-performance teams that consistently over-deliver. Creative, analytical, and adaptable, he drives change and efficiency, building lasting relationships with a "people do business with people" approach. With an exceptional track record of solving complex, cross-functional challenges on deadline, Edward is ready to deliver transformative security solutions for forward-thinking organizations.

Governance & Risk Assessment	Technical Security & Processes	Management, Leadership & Tools
IT / Security Budgetary Oversight	Continuous review and re-engineering of security controls and processes to efficiently reduce and manage risk	IT Infrastructure Management and Development
Framework / Regulatory Assessment & Compliance	Compensating and Mitigating Control enhancement recommendation	High-Performance Team Mentorship
- CCPA	Data Protection, Data Loss Prevention, and Encryption technology selection and implementation	Revenue Generation
- ISO-27001	Security control processes to integrate into the SWIFT, Fed-Wire, and CHIPS system	Program / Project Management
- GDPR	Identity & Access Management and Privileged User Access	Contract Negotiations

	strategy, technology, and implementation	
- ISO-27002	Practical Proof of Concept Testing	Budget Management for complex organizations in excess of $30M while achieving corporate objectives
- CIP	IT / Cybersecurity Consulting	Promoting OpEx savings through automation and staff efficiency
- FEDRAMP	Secure Development Lifecycle (SDLC) policy, process, and testing definition and management	Identifying redundancy and efficiencies between departments and areas of responsibility
- CIS	- Establishment of a policy and process framework for Secure Development Lifecycle	Streamlining and automating the response processes (removing HMI where possible)
- NISPOM	- Integration of standard security practices into the development objectives	IT & Security Tool Management
- NIST 800-53	- Track security in line with "bug" tracking	- Implementation
- NIST 800-61r2	- Establish security requirement tracking and testing regimen	- Business Rule Definition
- NIST 800-171r1	- Testing of security rigor at points in the SDLC commensurate to the development methodology	- Policy
- ISA/IEC 62443	Security Incident Response Management (holistically across the business and technology)	- Operational Sustainability
- NIST 800-82r3	Technology Assessments	- Configuration Management
Corporate-wide risk analysis; engaging Cybersecurity with business management and other stakeholders		Sample Technologies & Programs
Security Threat Profiling		- DLP, SEIM, SOAR, EDR, Penetration Testing, Forensic Analysis, eDiscovery
Creator of "Ransomware Resiliency and Protection Program (R2P2)" and assessment process		Strong interpersonal communication skills

Edward Liebig
liebig@wustl.edu

Threat Assessment and control gap analysis		
Emerging Cyber and business threat analysis		
Third Party Information Security Assessment Program management		

Edward Liebig
liebig@wustl.edu