

IT/OT Engagements

Edward Liebig MScIT/IA, CISSP, CISM

I recognize the challenge of sorting through the glut of applications and correlating experience against an open role. This document is supplied to illuminate my experience with IT/OT and various industry vertical environments.

I have built my career in IT from the ground up. In my early days, I worked across almost every role. In my service in the US Navy, I was awarded three Navy Achievement Medals (NAM) and was the Sailor Of the Year (SOY) for Pacific Operations Support Facility (1992). This dedication to duty and aptitude for technology has carried on throughout my rise to senior roles such as CISO and MssP/Professional Services Vice President/Managing Partner. I have a saying, "If you don't learn something every day, you aren't really in this business." I have kept up on the technological, architectural, and procedural advancements throughout the years and up to today.

I view the CISO role as focusing on the big picture of security strategy with and beyond technology (how to protect the business and brand while enabling the company to safely and dynamically flourish with minimal friction). The CISO role should help the CIO (driven by business objectives) shape the strategic IT and Security architecture while championing security processes and policy across business operations.

My IT and OT (manufacturing, Critical Infrastructure, Healthcare) experience may not be directly highlighted in my CV, so I am offering a bullet list of roles and client objectives for discussion starters from my engagements over the years.

- **Ajilon Consulting** – IT realignment and project direction over multiple industry verticals (telecommunication, Corporate Travel, Financial Services)
- **Manufacturers Life Insurance** (Manulife Financial) – IT realignment, security group/policy/process, and operations creation across the global matrix of 17 business units (Insurance, Banking, Annuities, and other financial service product lines)
- **CSC (now DXC) and Unisys** – In both roles, I owned the Professional Services consulting and Managed Security Service Provider (MssP) operations (Global SOC operations across multiple country locations). I was Core Creator of the "Protected Enterprise Assessment" (later changed to Enterprise Security Roadmap) and Creator of the CFATS assessment process

IT/OT Engagements

Edward Liebig MScIT/IA, CISSP, CISM

for the Chemical industry while assessing and measuring risk for all global plants DuPont. I was a core creator for a “consequence-based risk assessment” process. I applied this process across IT and OT for all Critical Infrastructure industries and was able to take this process to Unisys. I was the primary leader of the consulting practices in the CI sector for CSC and Unisys Corp.

- From the “executive interface” and team/program direction perspective, I led and amassed a team of vCISO level consultants to guide onsite activities for assessment and remediation activities across IT and OT for:
 - Huntsman Chemicals, Shell Oil, BAE Systems, Albemarle Corporation, Bombardier, General Dynamics (C4E and Electric Boats), Raytheon, UTC (and Pratt Whitney at the time), Wrigley’s, BMW, Chrysler, Ford, GM, DOT/RITA, United Coatings, General Electric, Delphi, Chevron, Exxon Mobile, National Grid/Keyspan, ConEd, Exelon, Monsanto, AT&T, Network Rail (EMEA), BHP Billiton (AU), Water Corporation (AU), Urenco/LES (EMEA), Maersk Oil (Qatar), VF Corporation, Bank Of New York, United Airlines, Commerce Bank, Master Card.
 - In the Healthcare vertical I lead teams to service the following clients:
 - St. Anthony’s hospital (now part of the Mercy Healthcare system) – physical build out and installation of networks and Datacenter (from wiring closets to servers)
 - Empire Blue Cross & Blue Shield – the production of and HCFA filing of BCP and DR planning for Y2K
 - Pace Health - Security review against HIPAA and HiTrust using the Enterprise Security Roadmap (ESR) methodology
 - Sutter Health - Security review against HIPAA and HiTrust using the ESR methodology
 - Cardinal Health – Security review against HIPAA and HiTrust using the ESR methodology

IT/OT Engagements

Edward Liebig MScIT/IA, CISSP, CISM

- Intermountain Health - Security review against HIPAA and HiTrust using the ESR methodology and program realignment/build out (two-year project)
- BioTech – AmGen - Security review using the ESR methodology and program realignment/build out.
- **Charter Communications** – through my work with Financial Services, I successfully identified the critical path technologies and processes (order to cash process) and applied PCI/DSS controls and policies/standards to ensure integrity, confidentiality, and availability.

Throughout the leadership of these engagements and the development of IT/OT processes, I had the opportunity to be a representative for CSC and Unisys in the ICSJWG (Industrial Control Systems Joint Working Group). I worked closely with Eric Cosman (President of ISA) in contributing and reviewing iterations of the early stages of ISA99 standards (later to become the IEC 62443 standard). I have been a long-time colleague and worked with Joe Weiss (ICS industry expert) in driving the position of ICS security as an industry voice. I worked with Dr. Kevin Morley at the American Water Works Association (AWWA) to examine and select a framework for the water industry. I partnered with CSC and MWH to create the Secure Water initiative (assessing the security of dams and water projects for cybersecurity vulnerabilities across IT and OT operations and architecture).

With this extensive manufacturing experience, coupled with my roles as CISO and corporate leadership, I stand ready to learn your environment and business to apply my lessons learned and perspective. In all my functions, I have done one or all the expectations below:

- Develop, implement, and monitor a strategic, comprehensive enterprise IT/OT cybersecurity program.
- Drive security standards across the organization, including information security policies and guidelines
 - Data privacy;
 - Data classification;
 - Endpoint security (EDR/XDR);
 - Training (end-user and IT/OT/Security Staff) and,
 - Testing (Tech POC, AppDevSec, etc.)
- Enhance an organization's ability to:

IT/OT Engagements

Edward Liebig MScIT/IA, CISSP, CISM

- Detect;
- Prevent;
- Mitigate; and,
- Respond to all security threats
- Work directly with the business units to facilitate risk assessment and risk management processes
- Led the architecture and engineering of new security systems, including evaluation of technical designs and pen testing
- Establish and maintain 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
- Establish Cross-Department/Division Incident Response process to recover and protect the business/brand from events
- Engage senior leadership across the organization to communicate the cybersecurity strategy and critical information security initiatives
- Provide guidance on information security topics, advising and collaborating on security processes, business continuity, and disaster recovery plans
- Provide leadership to the enterprise's information security organization, and lead day-to-day cybersecurity measures, investigations of any control failures, and continuous improvement initiatives
- Manage senior employee development by setting and evaluating goals, providing feedback, and employing development techniques to enable employees to realize their potential

I possess a bachelor's degree in Business Management (BScBM) and a master's degree in Information Technology with a specialty in Information Assurance and Security (MScIT/IA). I hold active CISSP and CISM certifications.

IT/OT Engagements

Edward Liebig MScIT/IA, CISSP, CISM

Thank you for taking the time to review this, and please let me know if I can offer any other support documentation to address your firm's current needs.

Sincerely,



Edward J. Liebig
MScIT/IA, CISSP, CISM
CEO, Yoink Industries LLC
ed@yoinkind.com
(636) 388-2625
<http://eliebig.com>
<http://linkedin.com/in/liebig>
ed@eliebig.com