Baird W. Brueseke, Principal
c – 858.232.4006
Baird.Brueseke@imergeconsult.com

OVERVIEW	Mr. Brueseke has over twenty years' experience in ECM and business process redesign, the last ten working on Cybersecurity projects. Mr. Brueseke focuses on helping organizations define the control framework appropriate to their organization, evaluate their security posture relative to those controls and prioritize remediation activities based on assessments of people, process and technology. Mr. Brueseke has worked with organizations such as San Diego Health Connect, Antelope Valley Hospital, Anchor General Insurance Company, Mitsubishi UJF Trust & Banking, Hewlett Packard, the Air National Guard and others including clients in health, finance, education, and multinational corporations. Mr. Brueseke's diverse experience in business and computing environments, forms processing, and Cybersecurity gives him a unique perspective on business problems with insight into creative ways of solving them. Mr. Brueseke specializes in assisting clients through the process of control framework selection, GAP analysis, security assessment, vendor selection and remediation planning.
CONSULTING PROJECTS SAN DIEGO HEALTH CONNECT Better Information • Better Care	San Diego Health Connect (SDHC) is the regional Health Information Exchange (HIE) for San Diego and Imperial Counties. Chartered under the guidelines established in the Health Information Portability and Accountability Act (HIPAA), SDHC facilities the exchange of electronic health records (EHR) between the major hospitals and physicians' groups serving over 1.3 million people. The information exchange is facilitated by a data center located 90 miles away in Costa Mesa using HL7 data streams displayed in a browser interface. Mr. Brueseke was concerned about the safety of his own medical information in the cloud and so he developed a proposal to perform a comprehensive Security Assessment on SDHC's business processes and technical infrastructure. The Security Assessment project had multiple components including: Technical Risk Assessment, Information Security Risk Assessment, Social Engineering, Vulnerability Assessment, Penetration Test, OWASP Assessment, Incident Response Policy Analysis and HIPAA Compliance Assessment. Deliverables included Executive Summary, color coded charts depicting risk levels, vulnerabilities ranked by severity and likeliness of exploitation, website coding issues, incident response timings, prioritized findings, commentary on employee behavioral patterns, a remediation plan and access to a HIPAA compliance tracking tool. MUFG Working with a large systems integrator, Mr. Brueseke's Cybersecurity Consulting Team was engaged to conduct a Security Assessment on Mitsubishi UJF Trust & Banking's (MUTB) New York City operations center. MUTB is a multinational banking enterprise which provides Investor, Asset Management and Real Estate services. In 2014 and again in 2015, Mr. Brueseke's team performed Security

	Assessments which provided MUTB executives with insight into the Security Posture of their network infrastructure. Anchor General Insurance Agency is a San Diego based company with 240 employees specializing in non-standard private automobile insurance in California, Texas, Oregon and Washington. Anchor's customers typically make their payments monthly, using credit cards via a website developed by an inhouse programming team. In 2015, Anchor's Attorney recommended that Anchor obtain Cybersecurity Insurance to provide coverage in the event of a data breach. As a pre-condition to obtaining this coverage, it was necessary to obtain an independent, 3rd party Security Assessment. Mr. Brueseke's Cybersecurity Consulting Team was engaged to provide this service. The project was completed in six weeks. Deliverables included a colorful Infographic which depicts the results of the GAP Analysis, a wall chart depicting Anchor's attack surface and internet footprint, Radar Charts which provide an analysis of people, process and technology for each of the CIS controls, a Vulnerability Assessment and Penetration Test Report with detailed findings and a Prioritized Remediation Plan.
EXPERIENCE	1990 to 2006. **EMC/Captiva Software**, co-founder Wheb Systems. Vice President. Mr. Brueseke designed the Intelligent Forms Processing System (IFPS). The first windows based system to use neural networks (ICR) to read hand printed forms. Wheb grew via VC funding, mergers and acquisitions to become Captiva Software, a public company purchased by EMC in 2005. 2008 to 2017. **iNetwork, Inc.** Vice President. Mr. Brueseke was responsible for Cybersecurity Projects at financial institutions, insurance companies, and healthcare organizations. In 2013, Mr. Brueseke participated in the NIST workshops @ UCSD and provided real-world input for the initial version of the NIST Cybersecurity Framework. Mr. Brueseke joined **IMERGE** as a Principal in 2017.
EDUCATION	BA, Elmhurst College
CERTIFICATIONS	Enterprise Content Management Practitioner, AIIM Certified Document Image Architect, CompTIA Company of Fellows # 185, AIIM
SPEAKING	Baird has spoken to many ARMA and AIIM chapters on topics including forms processing, business process re-engineering and Cybersecurity.
PROFESSIONAL	Mr. Brueseke is a member of the Association for Information and Image Management (AIIM) since 1991. His other activities include the Association of Information Technology Professionals (AITP), the High Technology Crime Investigation Association (HTCIA) and the Information Systems Security Association (ISSA).