Jeffrey D. Crump, CISSP, PMP, CSM, C^{2}MP^2
Mesa, Arizona USA
Jeff@JeffreyDonCrump.com | +1 (602) 821-5131

OVERVIEW:

Accomplished leader with a history of identifying, development and implementing solutions to help organizations reduce cyber risk and build resilience.

SELECTED ACCOMPLISHMENTS:

Led business/security-aligned initiatives to fundamentally transform how cyber risk is identified, managed and achieved including:

- Author, *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience*
- Led the development and validation of cyber crisis management plans for entities in the United States, China, Canada, Mexico, Russia, and India
- Led the development of information technology and information security policies and standards for Chinese joint venture.
- Led multiple core security capability program workstreams (internationally) for Deloitte & Touche to develop strategically aligned shared cyber risk services to meet five-year global revenue goals
- Led multiple capability gap analyses and resulting strategic roadmaps, the most current being the assessment of and resulting optimized supply chain security program for Intel, including sub-fab industrial control systems

PROFESSIONAL EXPERIENCE:

5/2017 – Current
Cyber Security Training & Consulting LLC
Phoenix, Arizona USA
Principal Consultant

- Cyber Crisis Management
  - Developed the Cyber Emergency Response Plan (CERP) for Express (Hangzhou) Technology Services Co. (American Express joint venture with LianLian)
  - Developed the Cyber Crisis Response Plans for American Express banks in USA, Canada, Mexico, India, and Russia
  - Assessed cyber crisis exercises for the Express (Hangzhou) Technology Services Co. and three American Express banks (Mexico, India, and Canada)
  - Achieved independent quality certification by PECB Management Systems of the Cyber Crisis Management Planning Professional course I developed
  - Authored Concept Note to address the implementation of cyber crisis management and information sharing capabilities for the U.S. Agency for International Development Europe and Eurasia
- China Cyber Security Law and Regulations
  - In support of operating license and China National Security Review requirements, serve as subject matter expert to American Express regarding China's cyber security laws and regulations

        - Developed the policy framework for information technology and information security risk management policies and standards for American Express' joint venture in China
        - Mapped China legal and regulatory controls to each other to identify overlap (e.g. GBT 22239, JRT 0071/0072, JRT 0142, China Cybersecurity Law, Cross-Border Data Transfer, Personal Information Standard, etc.)
        - Worked with China-based resources to develop an Information Security Management System (ISMS) to comply with ISO 27001 requirements
        - Mapped American Express policy and standards requirements to Joint Venture's ISMS library of measures and standards
        - Mapped China UnionPay Data Security Standards (UP DSS) for credit card processing to Payment Card Industry Data Security Standards (PCI DSS)
        - Consult on product selection for compliance with China's national requirements for encryption and security tools and technologies
        - Participate in product implementation validation and operational readiness reviews
        - Developed a Creative Commons licensed financial regulatory tool to be used by a lead assessor during a Hong Kong Monetary Authority (HKMA) Cyber Fortification Initiative (CFI) Cyber-Resilience Assessment Framework (C-RAF) Inherent Risk Assessment (IRA) and Target/Minimum Maturity Assessment (NIST/ISO 27002/FFIEC-based)
- Cyber Security Training
    - Developed the Capability Maturity Model Certification (CMMC) training course series designed form Level 2 – Level 5 defense industrial base contractor companies
    - Developed the *60 Seconds of Cyber* security awareness training course series
- Security Research and Contributions
    - Provide subject matter expertise on security and privacy standards and best practices through the development of executive and professional security awareness and training programs delivered to clients/employees such as IBM XForce Incident Response, KPMG, the OCC (Options Clearing Corporation), Indonesia's National Cyber and Cryptography Agency (BSSN), Saudi Arabia's King Abdulaziz City for Science and Technology, Hong Kong CITIC Bank, and Bank of America, including: Executive Education, Introduction to Cybersecurity Boot Camp, Cyber Crisis Management Planning Professional (C^2MP^2) Certification Boot Camp, and the FFIEC & ISO 27001/27002-based Hong Kong Monetary Authority (HKMA) Cyber Resilience Assessment Framework (C-RAF)
    - Conduct security research and publish public blog entries related to cybercriminal offender profiling with emphasis on the relationship between cultural factors (e.g. Hofstede's Nation Culture, United Nation's Cybercrime Law status, World Justice Project Rule of Law, poverty, etc.) and psychological factors (e.g. Hare Psychopathy Checklist Revised, Myers–Briggs Type Indicator, IBM Watson Personality Insights artificial intelligence, and the Java Graphical Authorship Attribution Program (JGAAP) and JStylo to leverage machine learning algorithms to identify threat actors)
    - Authored article on security awareness in Human Resources Magazine, the printed and online publication from the Hong Kong Institute of Human Resource

Management (HKIHRM)
- Authored article for the published Crisis Response Journal on cyber crisis leadership training challenges and the utility of virtualized environments as a viable option
- Article author of How China, Iran, and Russia Have, Are, and Will Attack the US, published on Medium, which provides summary analysis of MITRE ATT&CK™
- Authored a three-part article series on Cyber Threat Actor Cultural and Psychological Factors
- Authored article on the top tactics and techniques utilized by China, Iran, and Russia for cyberattacks against the United States, as per the MITRE ATT&CK data set

10/2014 – 5/2017
Deloitte & Touche LLP
Phoenix, AZ
Manager, Cyber Risk, Audit & Enterprise Risk Services

- Developed a Cyber Crisis (Management) Response Plan (CCRP) for an American multinational financial services client
- Led multiple international teams as part of a global operational change initiative (~$21M annual budget) to plan, build and run the Unified Cyber Portal (integrated applications and managed services) including Threat Service (Splunk & Jira-based Monitored Security Services Provider (MSSP), Threat Intelligence & Analytics, Global Application Security Testing (SAST, DAST, & MAST), Threat Lifecycle Management and Cyber Strategy (compliance assessment) Framework
- Collaborated with Global Cyber Executive Committee members, regional leaders (Americas, EMEA and APAC) and other member firm cyber leaders from locations such as the United States, Canada, Spain, Belgium, United Kingdom and Australia
- Liaised with, and develop reports for, multiple governance, risk and compliance bodies to comply with national and international standards
- Built and led a Global Cyber Rapid Deployment Team, responsible for the on-boarding of international member firms to the above-mentioned solutions. This included the development of an on-boarding artifacts ranging from an introductory primer to introduce global cyber leaders to the on-boarding process, kickoff and technical working session materials, global on-boarding project plan, detailed step-by-step process for on-boarding each capability, implementation of a centralized repository of all on-boarding materials, service catalog, interim support model, and vendor and interfirm legal/contracts
- Led a Supply Chain Security Program and Ecosystem assessment for a multinational semi-conductor client, which included conducting more than 20 interviews and related information security policies, procedures, standards, and guidelines and supplier contract reviews to assess the organization against eight domains:
    - Governance & Risk Management, Business Continuity, Human Resource Security, Identity & Access Management, Information & Asset Management, Physical & Environmental Security, Third & Fourth Party Security, and Threat Intelligence & Analytics
    - Also included an evaluation of the sub fab and building management system industrial control system (ICS) environments
    - Identified the need for specific security policies, procedures, standards, and

guidelines updates, and made recommendations to client regarding update approvals, dissemination, and maintenance

7/2014 – 10/2014
Wells Fargo
Phoenix, AZ
Contract Senior Project Manager

- Responsible for project to mitigate IRA fraud loss through procedural-based solutions

4/2013 – 7/2014
DataShield (now ADT Cybersecurity) Monitored Security Service Provider (MSSP)/Security Operations Center (SOC)
Scottsdale, AZ
Program Manager, Security & Compliance

- Worked with 40+ clients to identify, evaluate, and report on information security risks, practices, and controls required to mature their security and enhance overall resilience and compliance (e.g. GLBA, PCI, HIPAA HITECH, etc.)
- Primary point of contact for all client relationships, including the liaison between the customer and the Security Operations Center/MSSP
- Partnered with architects, infrastructure, and application teams to ensure that technologies and monitoring solutions complied with internal and client standards
- Led daily morning standup meeting with Security Operations Center staff
- Led the development of the Monitored Security Service Provider (MSSP)/Security Operations Center (SOC) Use Case Maturity Model (SOC-UCMM) framework, incorporating SANS Critical Controls, PCI, ISO 27001 and NIST Improving Critical Infrastructure Cybersecurity Executive Order 13636
- Established previously non-existent standardized processes for:
    - RSA Security Analytics Security Information and Event Management (SIEM) for (Packets), Envision (Logs), Event Stream Analyzer (Complex Correlation), and Data Loss Prevention client on-boarding
    - Develop metrics and dashboards for our internal staff and clients to measure and communicate the effectiveness of the security monitoring program, and increase both our internal and client's maturity of the program over time
    - Developed key artifacts for customer relationship management and operational effectiveness to include:
        - Monitored Security Service Getting Started Guide;
        - Client Security Profile (Organizational and Environmental factors);
        - Communication Plan;
        - Customer Configuration;
        - IPSec Connectivity Form; and
        - Monthly Executive Summary.
    - Developed and delivered program management data used in meetings with prospects and investors
- Led the preparation activities leading up to a Service Organization Controls Type 2 (SOC 2 Type 2) audit

10/2011 – 4/2013
Wells Fargo
Phoenix, AZ
Contract Senior Project Manager

2/2010 – 10/2011
CDI
Corporation
Phoenix, AZ
Client Executive

5/2008 – 2/2010
Symantec Corporation
Phoenix, AZ
Security & Availability Business Critical Account Manager

7/2007 – 5/2008
Compuware
Corp.
Phoenix, AZ
Senior Project / Program Manager

2/2007 - 7/2007
Keane, Inc.
Phoenix, AZ
Client Manager / Program Manager: Outsourced Services

2/2004 - 2/2007
EnterpriseCM, Inc.
Phoenix, AZ
Senior Project Management Consultant

10/1998 - 2/2004
SERENA Software, Inc.
Phoenix, AZ / Crossville,
TN
Managing Principal
Principal Change Management Consultant (Practice Manager)
Senior Change Management Consultant (Project Manager)

6/1996 - 10/1998
McKesson HBOC Phoenix, AZ
Project Manager

6/1992 - 6/1996
U.S. Coast Guard St. Petersburg, FL / Juneau, AK
Public Affairs Specialist / Project Manager

6/1984 - 6/1992
U.S. Air Force / First Colony Life / Bell Atlantic /
Ameritech Florida / Virginia / Pennsylvania / Illinois
Systems Programmer

EDUCATION:

- SANS ICS410: ICS/SCADA Security Essentials (Industrial Control Systems)
- Certified Cyber Crisis Management Planning Professional (C^2MP^2) Instructor
- Certified Information Systems Security Professional (CISSP) #548344
- Certified Project Management Professional (PMP) #418108
- Certified Scrum Master (CSM)
- COBIT Foundations
- ITIL Foundations Certified
- Graduate, Defense Information School (DINFOS)

SELF-PUBLISHED WORKS:

- Book author of *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience* available for sale on Amazon
- Article author of *How China, Iran, and Russia Have, Are, and Will Attack the US,* published on Medium
- Authored a three-part article series on *Cyber Threat Actor Cultural and Psychological Factors*
- Article author of *Myers-Briggs Type Indicator for Cybercriminal Psychology Offender Profiling*
- On-going series author of *Doxxing the Puppet*, which describes my personal account of using open source intelligence to (possibly) identify one the world's most wanted hackers, Phineas Fisher
- Article author on security awareness for Human Resources Magazine, the print and online publication from the Hong Kong Institute of Human Resource Management (HKIHRM)
- Article author of *Creating leaders on the cyber battlefield* for the print and online publication, Crisis Response Journal