3-DAY CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C^2MP^2) IMMERSIVE BOOT CAMP

WHEN & WHERE

2019

October 15-17: Phoenix, Arizona, USA
December 17-19: London, United Kingdom

2020

January 21-23: Los Angeles, California, USA
February 18-20: Bangalore, India
April 28-30: Chicago, Illinois, USA
June 23-25: Sydney, Australia
October 27-29: Orlando, Florida, USA
December 15-17: Madrid, Spain

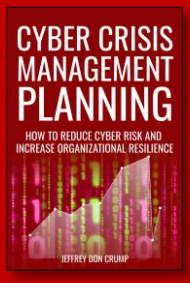
Core Topics (See detailed daily agenda on page 3)

- Foundations of Incident Response Planning
- Foundations of Cyber Crisis Response Planning
- Cyber Crisis Response Plan Development
- Cyber Crisis Response Plan Usage
- Cyber Crisis Response Plan Testing / Validation (Tabletop War Games)

INFO / REGISTER

W: CyberSecurityTrainingCo.com

E: Info@ CyberSecurityTrainingCo.com



Each student receives a free copy of *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience*

DESIGNED FOR MEMBERS OF THE CISO ORGANIZATION AND KEY BUSINESS STAKEHOLDERS

OBJECTIVE

A deep, hands-on immersion into the development of a Cyber Crisis Management Plan, which like a major cyber event, requires the collaboration of both line of business leaders and their partners in information technology / information security.

VALUE

During the fog of war (cyber crisis) is not the time to figure out how to respond. An effective response requires careful planning across an organization. This in-depth, hands-on, immersive boot camp gives attendees the knowledge and tools to complete their own CCRP.

TICKETS

Early Bird: US$ 2,750
General: US$ 3,500

INCLUDES

Buffet lunch
Break snacks
Coffee/Tea/Water

CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C^2MP^2) CERTIFICATION

Organizations globally are under constant attack from internal and external threat actors but often have blind faith that their information technology (IT) department's incident response plan will be adequate to address the response and recovery requirements for the entire organization.

As a certified Cyber Crisis Management Planning Professional (C^2MP^2) you will have the knowledge to help organizations prepare for a major cyber crisis by leading the development of an integrated plan that serves not only IT but also functional business and operational groups required to maintain resilience.

NOTE 1:

All three of the certification steps will be completed during the boot camp.

NOTE 2:

Students should expect to spend 2-4 hours working after-hours to complete classroom assignments.

NOTE 3:

Due to the time required to complete both the exam and the plan evaluation, students are advised to not schedule return flights home prior to 8 p.m.

STEP 1: TRAINING

C^2MP^2 candidates are required to attend our public or private Cyber Crisis Management Planning Boot Camp. This immersion course covers all facets required to pass the certification exam.

STEP 2: EXAM

Achieve a score of 70% or better on the C^2MP^2 exam

- 50 multiple choice questions
- Two hours; delivered on the final day of the boot camp
- Only material produced by the candidate during the boot camp are permitted as reference material during the exam

There is an exam re-take fee of US$449 for students who do not pass the exam on first attempt.

- One week must pass prior to attempting an exam re-take

STEP 3: PLAN EVALUATION

The Cyber Crisis Management Plan (CCMP) developed during the exam will be reviewed and evaluated based on the criteria below. A score of 80% or better is required.

- Presentation (15% of score)
- Structure (20% of score)
- Completeness (30% of score)
- Content (35% of score)

3-DAY CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL IMMERSIVE BOOT CAMP
DAILY AGENDA

IMPORTANT NOTES:

- ***This is a highly interactive, hands-on, immersive working course***
- ***Students should expect to work after-hours to ensure they are on-track with material development***
- ***A laptop computer is required***
- ***Microsoft Word, Excel, and PowerPoint are required (or equivalent technologies)***

DAY 1: FOUNDATIONS OF A CYBER CRISIS MANAGEMENT PLAN

- THE PLAN CORE
  - Acronyms
  - How to Use the Cyber Crisis Management Plan
  - Define Plan Purpose
  - Response Organization
  - Response Structure
- FUNCTIONAL INCIDENT RESPONSE PLANS
  - Functional Incident Response Plan (Detailed)
  - Functional Incident Response Plan (Summary)
  - Linking Incident Response Plans
- RESPONSE PROCESS FLOW
  - Response Process Flow Foundation
  - Master and CSIRT Incident Response Plans
  - Response Process Flow Completion
- CYBER WAR ROOMS & BRIDGE LINES
  - War Rooms
  - Bridge Lines
  - Cyber Crisis Logistics
- TEAMS, ROLES & RESPONSIBILITIES
  - Cyber Crisis Executive Team (CCET)
  - Cyber Crisis Management Team (CCMT)
  - Cyber Crisis Response Team (CCRT)
  - Computer Security Incident Response Team (CSIRT)
  - Cyber Crisis Support Team
- WORKING GROUPS
  - Communications Working Group
  - Technology Working Group
  - Additional Working Groups

DAY 2: CYBER CRISIS MANAGEMENT ROLES, CHECKLISTS & TEMPLATES

- PLAN OWNERSHIP AND GOVERNANCE
  - Plan Ownership
  - Plan Governance
- IMPACT CATEGORIES, SCALES & SCORES
  - Impact Categories, Scales & Scores Table
- CYBER ATTACK & CRISIS ANATOMIES
  - Cyber Attack Anatomy
  - Cyber Crisis Management Anatomy™
- CYBER CRISIS INFORMATION FORM
  - CCIF Development
- CHECKLISTS
  - Lead Incident Handler Checklist
  - Pre-Confirmation
  - Post-Confirmation
  - Cyber Crisis Deactivation Checklist
- TEMPLATES
  - LIH-to-EIC Email Template
  - EIC-to-CCRT Incident Notification Email Template
  - LIH-to-CCRT Initial Meeting Email Template
  - Initial CCRT Meeting Agenda Template
  - Subsequent CCRT Meeting Agenda Template
  - SEIC-to-CCET Email Template
- QUICK REFERENCE CARDS
  - CCET Quick Reference Card
  - SEIC Quick Reference Card
  - EIC Quick Reference Card
  - LIH Quick Reference Card
  - IRL Quick Reference Card

DAY 3: CYBER CRISIS MANAGEMENT/RESPONSE PLAN USAGE AND VALIDATION (TABLETOP WAR GAMES)

- PROJECT PLANNING
  - Project Resources
  - Project Phases & Activities
  - Phase I: Plan
  - Phase II: Build
  - Phase III: Test
  - Phase IV: Implement
- TRAINING THE ORGANIZATION
  - CCMP Training Deck
- TABLETOP CYBER WAR EXERCISES
  - Tabletop Exercises vs. Immersive Simulations
  - Exercise Roles & Responsibilities
  - Exercise Logistics
  - Exercise Materials
  - Exercise Execution
  - Exercise Conclusion
  - After-Action Reporting
- WRAP-UP
  - Version Control
  - Release Planning

Mr. Crump is the author of *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience* and Managing Director of Cyber Security Training Company. He is a former manager at Deloitte & Touché LLP Cyber Risk Services in the USA, the former Program Manager, Compliance & Security for Datashield Monitored Security Service Provider (now ADT Cybersecurity) and a former Symantec Business Critical Services Manager. He is a veteran of the US Air Force and US Coast Guard. His professional credentials include Certified Information Systems Security Professional (CISSP), certified Project Management Professional (PMP), certified Scrum Master (CSM), and is ITIL Foundations certified.