CYBER CRISIS RESPONSE
A SERVICE OF CYBER SECURITY TRAINING AND CONSULTING LLC

CYBER CRISIS MANAGEMENT

THE COMPANY
Mesa Center for Higher Education | Arizona

THE CAPABILITIES
Innovative Cyber Risk Solutions
In 2014, American Express wanted to improve its incident response capability. As a cyber risk consultant, Jeffrey Crump advised the financial services giant it needed to transition to a holistic view of incident response, to evolve into a new domain: cyber crisis management.

Since that time, Mr. Crump authored a step-by-step book on the framework and developed a cyber crisis management planning certification course. In 2019, Mr. Crump led the development of a cyber emergency response plan for the American Express/LianLian joint venture in China, and in 2020, integrated their banks in the USA, Canada, Mexico, Russia, and India into the enterprise model.

When a major cyber incident strikes, the effects extend well beyond the traditional boundaries of information technology (IT). As such, tech-centric incident response (IR) plans fall short. The solution is a cross-organizational, integrated cyber crisis management plan (CCMP).

Since that time, Mr. Crump authored a step-by-step book on the framework and developed a cyber crisis management planning certification course. In 2019, Mr. Crump led the development of a cyber emergency response plan for the American Express/LianLian joint venture in China, and in 2020, integrated their banks in the USA, Canada, Mexico, Russia, and India into the enterprise model.

When a major cyber incident strikes, the effects extend well beyond the traditional boundaries of information technology (IT). As such, tech-centric incident response (IR) plans fall short. The solution is a cross-organizational, integrated cyber crisis management plan (CCMP).

- "The regulators love it!" Director, American Express
- Reserve Bank of India circular RBI/2015-16/418 states, "A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy."
- Clear indicators from multiple regulators requiring cyber crisis capabilities & board integration

3 STEP PROGRAM

01 DEVELOP PLAN
Roles, responsibilities, activities, logistics, and so much more

02 PREPARE LEADERS
Build effective leadership mental muscle memory before the crisis

03 TEST & OPTIMIZE
Identify what’s right, what’s wrong, and what could be better
As the author of the CCMP framework, we have a deep appreciation for the value and reliability a standardized approach provides. This framework affords the ability to streamline CCMP development and implementation. At the same time, a framework must be flexible to allow for the unique requirements each customer brings to its structure.

The CCMP has a core, the information that needs to be comprehended in short order. This core is how we make a large plan consumable by the audience. We also bring a set of templates and checklists, which can be reused as they are but customers are encouraged to customize them. These valuable assets are exclusive to our service and we customize them to your organization.

During the CCMP development process, key stakeholders across the organization are exposed to the plan. However, exposure is not the same as education so we address this during the project. And, education is not the same as usage. Therefore, we work with organizations to plan and execute a series of paper-based tabletop exercises, which reinforce plan usage and validate its contents. Our Cyber Crisis Management Exercise Professional (C2MEP) certification course combines lecture with practicals to ready them for developing, leading, and assessing cyber exercises.

Those tasked with the critically important role of leading a cyber crisis response have unique education and training requirements. Our industry-exclusive Cyber Crisis Management Leadership Professional (C2MLP) certification course is designed to ensure these leaders are poised for success.

---

**STANDARDIZED, REPEATABLE, FLEXIBLE**

**PLAN VALIDATION**

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

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 immersion boot camp gives attendees the knowledge and tools to complete their own CCMP.

**COURSE OUTLINE**

**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

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
CERTIFICATION COURSE

CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C2MP2)

COURSE OUTLINE (CONTINUED)

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

CYBER CRISIS MANAGEMENT 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
The objective of this service is to immerse an organization’s cyber crisis leadership team into a real-world like integrated education, analysis and performance optimization experience designed to prepare the team to effectively lead the response to a major cyber incident.

Cyber crisis leaders graduate from the course with new-found knowledge, confidence, and capabilities uniquely designed to prove to the board, regulators, customers and shareholders that the organization is committed to doing all it can to reduce cyber risk and increase organizational resilience.

**COURSE OUTLINE**

**BECOMING A SENSEMAKER**
- The Leadership Challenge
- Identifying the Root of Poor Crisis Management
- Cyber Crisis Management Leadership Range: Online Situational Immersion 1
- How Sensemaking Works
- The Value of Accuracy and Incremental Clarity

**CLUE RECOGNITION**
- Exploring the Wider System
- Creating Situational Maps
- Clue Overload
- What You See is All There Is
- Blind to the Obvious | Blind to our Blindness
- The Power of Recognition
- Three Common Heuristics
- Cyber Crisis Management Leadership Range: Online Situational Immersion 2
- Cyber Crisis Management Leadership Range: Online Situational Immersion 3
- Multinational Cross-Cultural Considerations | Cyber Attack Data Correlation
- Top Techniques Used by Advanced Persistent Threats (APTs): China, Iran & Russia
- Visual Influences on our Intuition
THINKING IN FRAMES

- Magic Andrea
- Frames
- Recognition-primed Decision Making
- Influential Cyber Risk Frames
- Cyber Crisis Management Leadership Range: Online Situational Immersion 4
- Cyber Crisis Management Leadership Range: Online Situational Immersion 5
- The Professional Risk Frame
- (Re)Framing to Remove Blind Spots
- Tools in the Kit
  - Perspective-taking
  - Issue Selling
  - Effective Communications
  - Creativity
  - Organizational Agility
  - Risk Taking
- Leveraging the Gift of Fear
- Surviving a Trip to the Edge of Chaos
- Dressing for Success | Employing the Bowtie Model
  - Factoring Impact Categories, Scales & Scores

CAPABILITY INTEGRATION

- Magic Andrea: Sharing her Secrets
- Change the System from Within | Tools for Change
- Exercises for Mental Muscle Memory
- After-action Reviews
- Giving Honest Performance Feedback to Leaders
CERTIFICATION COURSE

CYBER CRISIS MANAGEMENT EXERCISE PROFESSIONAL (C2MEP)

OBJECTIVE
An immersion into planning, developing, conducting, and assessing tabletop cyber war games that are aligned to and compliant with the U.S. Homeland Security Exercise and Evaluation Program (HSEEP). Although there is no such thing as being “HSEEP certified” this course will certify students do indeed understand and apply the FEMA program as it is aligned to the cyber security domain.

COURSE OUTLINE
FOUNDATIONS OF TABLETOP CYBER WAR EXERCISES
- Tabletop Exercises vs. Immersive Simulations
- Exercise Scope
- Exercise Design & Development
- Setting the Foundations
- Planning Meetings
- Concept and SMART Objectives Meeting
- Initial Planning Meeting
- Midterm Planning Meeting
- Master Scenario Events List Meeting
- Final Planning Meeting
- Exercise Roles & Responsibilities
- Exercise Execution & Logistics
- Exercise Materials
- Situation Manual
- Player Handbooks
- Facilitator Guide

VALUE
The ability to plan, develop, deliver, and assess tabletop war games are essential skills required to validate an organization’s incident response and cyber crisis management plans. Acquiring this certification demonstrates a unique and specialized set of knowledge, skills, and abilities.
COURSE OUTLINE (CONTINUED)

- Exercise Presentation
- Exercise Evaluation Guide
- Participant Feedback Form
- Exercise Conclusion
- After-Action Reporting
- Exercise Improvement Planning

TABLETOP CYBER WAR EXERCISE PRACTICALS

- Assignment
- Develop all contents required to build, deliver, and assess an exercise
- Practical
  - Serve as facilitator for a given exercise subset
  - Act as observer for a given exercise subset
Cyber crisis readiness helps reduce chaos by establishing a plan, building awareness of the plan, refining crisis leadership confidence and capability, and optimizing for excellence and cyber crisis management maturity.

the project sponsor sets the tone across the organization by communicating the importance and value of creating a cyber crisis management plan
LET'S GET STARTED

Contact us today to receive a no-obligation, no-cost services and/or education quote.

CYBER SECURITY TRAINING AND CONSULTING LLC
245 West 2nd Street
Suite 027
Mesa, AZ 85201
CyberCertify.me
CMMCTraining.Academy
CyberCrisisResponse.com
CyberSecurityTrainingCo.com

MESA CENTER FOR HIGHER EDUCATION

East Bound & West Bound
Stop #18601
Country Club/Main Street