2007 CHS National Conference
Answering the Call—Professional Practitioners in Homeland Security

Hyatt Regency - Crown Plaza, Kansa City, MO – October 2-6, 2007

Tuesday, October 2nd

3:00 – 5:00 p.m. National CHS- NERT Meeting *(2 CE Credits)*
6:30 – 9:00 p.m. Welcome Reception *(2 CE Credits)*
7:00 – 8:00 p.m. Welcome, CAO, Marianne Schmid & Chair John Bridges, III
8:00 – 9:00 p.m. **Key Speaker Wm. R. Spernow**

Wednesday, October 3rd

7:00-8:00 am Registration/Continental Breakfast
8:00 – 8:15 am Announcements *(2) CE Credits*
8:15 – 9:45 am Meet the CHS Board Members
9:45 –10:00 am Morning break
10:00–11:00 am Presentations
11:15-12:15 pm Presentations
12:15-1:15 pm Lunch on your own
1:15-2:15 pm Presentations
2:15-3:30 pm Presentations
3:30-3:45pm Afternoon Break
3:45-4:45 pm Presentations
6:30 -9:00 p.m. CHS Awards Banquet (3)CE's available **Key Speaker: Dr. Sidney Niemeyer**

Thursday, October 4th

7:00-8:00 am Continental Breakfast
8:00-9:00 am Presentations
9:15-11:00 am Presentations (10:00-10:15 Break)
11:15-12:15 pm Presentations
12:15-1:15 pm Lunch on your own
12:15-2:15pm Presentations
2:15-2:30 pm Afternoon Break
2:30-4:30 pm Presentations

1:15-2:15 (Chouteau B)
Information Security
John F. Petrie, CHS-III
This presentation will identify an alternate organizational structure for combating cyber attacks and help attendees understand the centralization of security resources, identify some ROI metrics that can support their organizational designs, and understand the effect of a strategic information security plan on the corporate culture and the ability to create change.
(1) CE Credit

Abstract

Title:

Information Security:

Organizing for the future – Centralizing Resources to Combat Cyber Attacks

Time: 1.5 hrs (90 min)
Instructional Method: Lecture
Audience: Leaders and Managers
Level of Instruction: Intermediate
Learning Objectives:

1. Identify an alternate organizational structure for combating cyber attacks
2. Understand the centralization of security resources
3. Identify some ROI metrics that can support your organizational design
4. Understand the effect of a strategic information security plan on the corporate culture and the ability to create change

Prerequisites: None
Advanced Preparation: None
Contact Information:

John F. Petrie III
Chief Information Security Officer
Clarke American Checks
(v) 210-697-1328
(f) 210-694-1435
jpetrie@clarkeamerican.com

Audio Visual Equipment: Overhead projector and screen, microphone (lapel), PowerPoint Presentation

Abstract:
This case study provides an alternate approach for companies to organize their limited security resources to become a force multiplier against cyber attacks. Regulatory restrictions impact all functional areas of the organization – these regulations are changing the way we do business. Recent events have caused us to look at the world differently. A vendor, supplier, manufacturer, or business can no longer be satisfied that their security programs, and the security controls associated with the program, are functioning correctly across the entire enterprise. The physical security and incident management can no longer operate in silos, nor can the security program as a whole operate with out a risk management framework. At the end of the day, Executive leadership and Boards of Directors must view security as an enhancement to their overall business strategy, and the must support the program. The information security function can be a productive vehicle to implement cultural change in process, people, and policy. The material presented shows unique ways to leverage resources (people, equipment, and money), time, and structure by implementing a comprehensive strategic information security plan.

John F. Petrie III
MBA, CISSP, CISM, CBM, CHSP, CHS-III
Chief Information Security Officer
Clarke American Checks
January 2006

Other key areas addressed in this presentation:

Policy
Organizational Structure
Supplier Management
Reporting
Centralized vs. Decentralized
Risk Management
Business Continuity and Recovery
Confidentiality, Integrity, and Availability
Sarbanes-Oxley Act
Gramm-Leach-Bliley Act (GLB)
Homeland Security
Critical Infrastructure
Public Key Infrastructure (PKI)
Incident Response