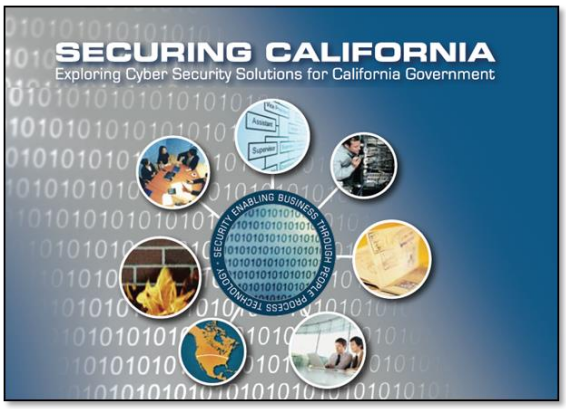
INNOVATIVE PRACTICE

Cybersecurity: California's Annual Cybersecurity Awareness Event

SUMMARY

The *Lessons Learned Information Sharing (LLIS.gov)* team identifies innovative practices within the whole community and documents these practices for emergency managers to consider for incorporation when developing plans and exercises. This document provides an example of how one state is bringing together whole community partners to address training gaps and improve cybersecurity awareness through an annual event.

The *LLIS.gov* team interviewed the State Chief Information Security Officer of California about their cybersecurity preparedness efforts—specifically their efforts to improve awareness of cybersecurity issues and threats.



California's annual cybersecurity awareness event brochure 2007, highlighting the theme "Securing California: Exploring Cyber Security Solution for California Government." *(Source: Email Interview with Michele Robinson, February 26, 2014.)*

The State of California participates in the Department of Homeland Security's (DHS) Stop.Think.Connect.™ Campaign as a member of the DHS Cyber Awareness Coalition and is actively involved in National Cyber Security Awareness Month activities each October. In addition, the State of California also hosts an annual cybersecurity awareness event that brings together whole community partners to provide education and training on cyber issues, threats, and response tactics. The Governor's Office of Emergency Services has served on the event's Advisory Board, reinforcing the connection between cyber preparedness and emergency response.

DESCRIPTION

Since 2007, the California Information Security Office (CISO) and its partners have hosted an annual cybersecurity awareness event to provide information and training to the whole community on cybersecurity threats. The goal of the event is to address cyber issues from an end-user perspective by providing access to whole community cyber experts and a forum for participants to discuss threats and improvements to cyber capabilities. The event attracts attendees and presenters from all levels of government, higher education, the private sector, utilities, and owners and operators of critical infrastructure. During the

event, participants identify and work to address capability gaps through information sharing, access to whole community cyber experts, and training opportunities. This event serves as one component of the state's cybersecurity training efforts, providing expert-led training and opportunities to practice skills needed to prevent, mitigate, and recover from cyber incidents.

Integrating Whole Community Input and Participation

The CISO conducts extensive outreach in order to encourage extensive whole community participation. Sixty-seven participants attended the initial event in 2007, which featured seven sessions. By 2013, the event had grown to feature 35 sessions—including panels, group discussions, and courses—and was attended by more than 500 emergency responders, security personnel, government officials, and cyber experts.

Since 2007, event organizers have also expanded the scope of the content for the event. As the event has expanded, organizers have worked closely with the whole community to ensure the event's agenda matches the participants' needs. To achieve this, the CISO and its hosting partners recruit representatives from all participating sectors to participate in the event's Advisory Board.

Developing the Advisory Board

The CISO develops the Advisory Board for its annual cybersecurity awareness event and ensures the Board includes representatives from all government, education, and critical infrastructure sectors involved in cybersecurity preparedness. The CISO seeks out Board Members who have responsibilities in the following areas:

1. Privacy
2. Information Security
3. Business Continuity and Disaster Recovery
4. Information Technology
5. Communications
6. Emergency Management
7. Legal
8. Law Enforcement
9. Health Care
10. Financial
11. Utilities

The CISO sends out invitations to potential Board members, working to balance representation between the stakeholder groups. If a sector is underrepresented, the CISO conducts additional outreach to stakeholders in the underrepresented group to identify and recruit suitable Board members.

The Advisory Board provides a platform for stakeholders to provide input and discuss the challenges they face in their unique sectors. Event organizers incorporate the Advisory Board's inputs into the agenda development process. This collaborative process ensures that the agenda reflects stakeholder concerns and addresses identified capability gaps.

Building Partnerships to Provide Expert Advice and Training

Whole community outreach is also an important tool for recruiting a diverse array of experts, speakers, and trainers for the event. Once event organizers set the agenda, they work with state agencies, private industry, and higher education partners to bring in cyber experts to provide information and training that addresses stakeholder concerns and cybersecurity preparedness gaps.

Organizers aim to provide content based on the specific interests and needs of various sectors, customizing sessions in order to provide the most effective training. Presenters adjust the level of technical detail of each event session to match the audience's familiarity with cyber issues. For example, in 2011, some event participants from the education sector expressed an interest in attending a session covering more technical aspects of cyber

preparedness. The CISO worked with private industry partners to bring in experts to provide detailed technical content for a presentation, helping meet the audience's needs.

Providing Specialized Training for Senior-Level Officials

Over the past three years, the CA annual event has included specialized cybersecurity courses to provide awareness and training for senior-level government officials, including the Governor's senior staff and state department leads. According to state IT officials, these senior staff members leave the events with a better understanding of the cyber issues and challenges facing their respective organizations. Moreover, participants have maintained engagement between their departments and IT officials post-event, seeking additional information on cyber threats and working to continue the dialogue on ways to mitigate cyber threats. California has worked with the DHS Office of Cybersecurity and Communications, which helps provide executive briefs and conducts training courses.

Organizers also recruit experts to speak at lessons learned sessions. One year, the event featured a panel of Chief Information Officers and Chief Information Security Officers from state, county, and local governments discussing lessons they had learned from past cyber breaches and incidents.

The CISO has also used this whole community-focused recruitment process to work with the emergency management community to provide content on emergency management capability gaps. In 2013, event planners worked with the Governor's Office of Emergency Services' Planning, Protection, and Preparedness Division to provide specialized content aimed at improving emergency response. This partnership coordinated with the Naval Postgraduate School to bring in one of the school's mobile education teams. The mobile education team conducted an Executive Educational Seminar, providing a half-day, interactive roundtable designed to improve executive capacity for incident response. Additionally, in 2013, the Governor's Office of Emergency Services served on the event's Advisory Board, reinforcing the connection between cyber preparedness and emergency response.

SUMMARY

California established a model for hosting a regularly scheduled cyber event to improve whole community cyber preparedness and response that can be replicated in other states and localities. This whole community engagement approach builds valuable partnerships that provide the collaboration needed to effectively shape the event agenda and meet event objectives. Additionally, these partnerships drive information and expertise sharing that helps all sectors better prepare for and respond to cybersecurity incidents.

REFERENCES

Center for Homeland Security and Defense – MET Seminars; The Naval Postgraduate School and the Department for Homeland Security. Accessed on February 18, 2014. http://www.chds.us/?met.

Michele Robinson, Chief Information Security Officer – California Information Security Office. Phone interview, February 7. Email interview, February 26, 2014.

Public Sector Partners – Advisory Board for Cyber Security Symposium 2013. Accessed on February 27, 2014. http://pspinfo.us/event-advisory-board/?event_id=320.