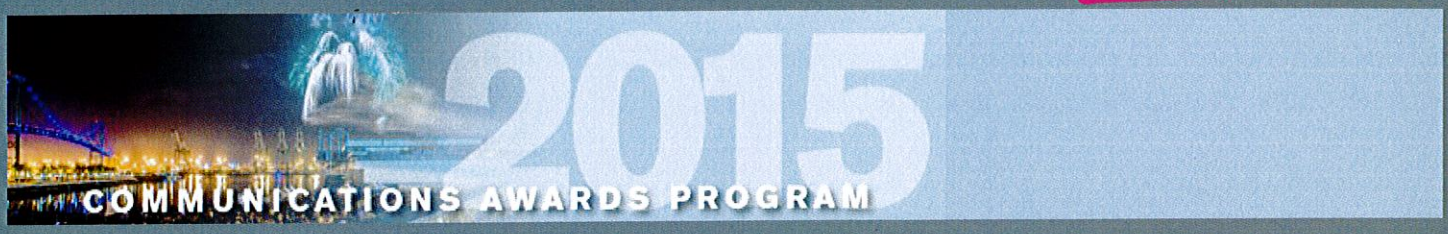
6081



2015 COMMUNICATIONS AWARDS PROGRAM

#9

INDIVIDUAL SUBMISSION ENTRY FORM

Please copy and complete this form for each entry.
Create a separate document for answering the five questions below.

Check only ONE entry classification below:

1.	AAPA Awareness Initiative Messaging	8.	Overall Campaign
2.	Advertisements – Single	9.	Periodicals
3.	Advertisements – Series	10.	Promotional/Advocacy Material X
4.	Annual Reports	11.	Social/Web-Based Media
5.	Audio-Only Presentations	12.	Special Events
6.	Directories/Handbooks	13.	Videos
7.	Miscellaneous	14.	Visual-Only Presentations
		15.	Websites

Please check the appropriate box:

☐ CATEGORY 1 ☐ CATEGORY 2 ☒ CATEGORY 3

Entry Title: **Cyber Security Employee Training**

Name of Port: Port of Long Beach

Port Address: 4801 Airport Plaza Drive

Contact Name/Title: Michael Gold

Telephone: 562 283 7711 Email Address: michael.gold@polb.com

On separate paper, **FIRST** write a short, descriptive summary of your entry, **THEN**, in as much detail as needed, specifically address each of the following five questions and number your answers. Your answers equal 50% of your score.

1. **What are/were the entry's specific communications challenges or opportunities?**
   - *Describe in specific & measurable terms the situation leading up to creation of this entry.*
   - Analyze the major *internal and external factors needing to be addressed.*
2. **How does the communication used in this entry complement the organization's overall mission?**
   - *Explain the organization's overall mission and how it influenced creation of this entry.*
3. **What were the communications planning and programming components for this entry?**
   - *Describe your overall goals or desired results.*
   - *Describe your objectives and list specific, measurable milestones needed to reach your goals.*
   - *Identify your primary and secondary audiences in order of importance.*
4. **What actions were taken and what communication outputs were used in this entry?**
   - *Explain what strategies were developed to achieve success and why these strategies were chosen.*
   - *Specify the tactics used (i.e., actions used to carry out your strategies).*
   - *Detail the implementation plan by including timeline, staffing and outsourcing used.*
5. **What were the communications outcomes from this entry and what evaluation methods were used to assess them?**
   - *Describe any formal/ informal surveys used, or anecdotal audience feedback received, that helped in evaluating the success of this entry.*
   - *If possible, explain how this entry influenced target audience opinions, behaviors, attitudes or actions.*

Summary:
Title: Cyber Security Employee Training

Classification: Pormotional/Advocacy Materials

Stop. Think. Connect. That was the advice to employees during the Port of Long Beach Cyber Security Awareness Program scheduled to coincide with National Cyber Security Awareness Month in October.

As reliance on information technology and data management continues to grow, cyber security has become more and more critical, and the program was designed to raise employees' awareness of the issue. Activities included a stealth attack on staff computers, leading to a simulated "cyber gotcha page" for those who used a fake flash drive, and a cyber workshop that featured an FBI special agent who focuses on cyber security issues.

Port of LONG BEACH
The Green Port

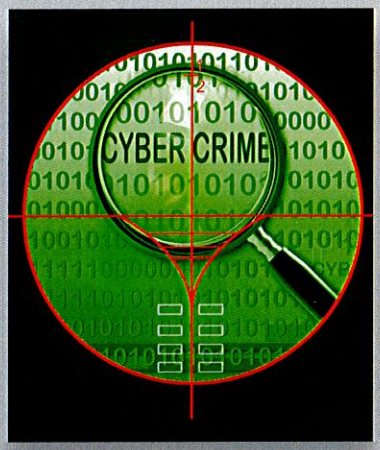
2015 AAPA Communications Awards

Classification: Promotional/Advocacy Materials

Title: Cyber Security Employee Training

Port of Long Beach
Cyber Security Employee Training

1. Communications Challenges and Opportunities



The Port of Long Beach is the premier U.S. gateway for trans-Pacific Ocean trade with Asia and a trailblazer in innovative goods movement, safety and environmental stewardship. As the second-busiest container seaport in the United States, the Port serves 140 shipping lines with connections to 217 seaports around the world. More than 40 percent of the nation's inbound cargo arrives through the ports of Long Beach and Los Angeles.

With annual trade valued at $180 billion, the Port of Long Beach is a major economic engine for Long Beach and the surrounding Southern California region, where more than 300,000 jobs are created due to the trade that passes through the Port. Business through the Port supports one in every eight jobs in Long Beach. That translates to 30,000 Long Beach jobs and expands to nearly 1.4 million jobs nationwide, with Long Beach trade goods reaching every U.S. congressional district.

The Port is a self-supporting part of the City of Long Beach and operates under the banner of the Harbor Department to serve the citizens of Long Beach, as well as its many Port customers and stakeholders.

The port industry is evolving rapidly, with major infrastructure and operational improvements to accommodate the bigger ships entering the trans-Pacific fleet. The Port of Long Beach is in the midst of a more than $4 billion capital improvement program, spending more than any other U.S. port, including terminal, channel, railroad, roadway and bridge improvements to support trade and jobs growth.

The gigantic new ships have brought about colossal change in the end-to-end movement of cargo, which has been partly responsible for congestion on the docks. The Port of Long Beach is currently addressing the need for systemic industry-wide change to achieve higher velocity and systems optimization in the big-ship era. The new model will be built around information technology and managing data to connect overseas vessel stowage offices, shipping lines, marine terminals, freight intermediaries, truckers and railroads in a single loop.

In a competitive world market, as reliance continues to grow on information technology and data management, cyber security has become more and more critical to uninterrupted operations.

A Nov. 12, 2014, news item in the Long Beach Press-Telegram reporting on a Port Security Operations Conference and Expo attended by various port and law enforcement agencies contained these quotes from various speakers:

- *"Cyber threat is no longer emerging, it's here."*
- *"My port gets about five hacker attempts per second."*
- *"There's been a growing number of disruptions in that area (cyber security). In recent years, that has included ... drug cartels hacking into shipping companies' computers to track and intercept drug shipments, password-cracking software, and a disgruntled employee who loaded malware into a refinery's system, taking down its business system for almost a week."*

The Port of Long Beach Cyber Security Program, managed by the Port's Information Management Division, is highly effective at protecting the Port

Port of LONG BEACH
The Green Port

2015 AAPA Communications Awards

Classification: Promotional/Advocacy Materials

Title: Cyber Security Employee Training

from cyber attacks.. The division promotes the message that protecting online Port information is everyone's responsibility.

About 350 of the Port's 500 staff members have direct computer access, and during National Cyber Security Awareness Month, they participated in an employee program designed to increase awareness and emphasize the importance of being vigilant online – and have some fun at the same time.

2. Complementing the Overall Mission

One of the Port's primary goals, a goal shared by harbor commissioners, executive management and staff, is to provide open channels of communication between the Port and its many constituents and target markets.

One target audience that is critically important to the smooth operation of the Port of Long Beach is the Port staff. These employees make the second-busiest container seaport in America "go."

The Port is spread over 3,230 acres with 31 miles of waterfront, and the various divisions that make up the Port's six bureaus – Commercial Operations, Communications, Finance and Administration, Engineering Services, Planning and Environmental Affairs, and Human Resources and Team Development – maintain communications links through a variety of Communications programs.

The Communications Division has established both a monthly employee newsletter (Dock Talk) and a weekly video news program for employees (POLB in 3), and it regularly works with other Port divisions to communicate news about their programs and activities to employees working throughout the Port. This cyber security awareness exercise, initiated by the Information Management Division, is a perfect example of that kind of collaboration.

3. Planning and Programming Components

The Information Management and Communications teams began with the mission of increasing overall exposure to and awareness of the importance of cyber security at the Port of Long Beach and the part all employees play in keeping the Port safe.

The primary target audience for this program was the Port's 500 employees, and the goal was to increase awareness of the Port of Long Beach Cyber Security Program among employees, therefore increasing the program's effectiveness.

To accomplish this, the Information Management and Communications teams prepared a 45-day timeline (mid-September through October), established a $5,000 budget for all activities, and developed a communications plan to engage the employees.

Activities would include:

Participation for the fifth year in National Cyber Security Awareness Month in October, with a goal of gaining a minimum of 70 percent participation in its organizational education and outreach activities. National Cyber Security Awareness Month (NCSAM) activities are managed by the National Cyber Security Alliance, whose mission is to educate and empower a digital society to use the Internet safely and securely at home, work and school, protecting the technology that we use, the networks they connect to, and our shared digital assets. The focus for 2014 was on three specific areas of concern: passwords, the Cloud, and what employees can do to stay safe online.

Port of LONG BEACH
The Green Port

2015 AAPA Communications Awards

Classification: Promotional/Advocacy Materials

Title: Cyber Security Employee Training

- A special guest speaker in a workshop setting.
- In keeping with the Halloween season, "tricks" in the form of fake cyber threats planted by IT to be resolved by employees, and "treats" for participating.

4. Actions Taken and Communication Outputs Used

"Stop. Think. Connect." was the headline for communications with employees about the Port's participation in National Cyber Security Awareness Month and the activities that would take place during the month of October. After two weeks of planning and preparation, the team followed this schedule:

September 30

A colorful announcement appeared in the employee electronic newsletter, Dock Talk, previewing the October activities with teases about upcoming "tricks" and "treats" and directing employees to more information via a link to the Port Intranet. The team then followed up with email blasts to staff.

October 3

The Information Management Division announced National Cyber Security Month in their Bureau Notes and then announced the results of the educational activity. Bureau Notes is distributed to Port staff weekly via email and contains updates on each bureau and division's activities and accomplishments.

October 9

The educational activity began when suspicious USB "flash" keys were distributed to all staff via interoffice mail. This resulted in 17 calls to the Information Management Service Desk and more than 100 USB keys being plugged in. The first few callers were given kudos for being among the first to pass the test by questioning the unidentified key and calling the Information Management Service Desk. When plugged in, the "flash" drive presented itself as a keyboard with a pre-recorded set of keystrokes that took the computer to a "cyber gotcha page." This activity demonstrated the importance of having non-Port-issued items checked out by the IM Service Desk before use.

October 10

The Information Management Division announced the results of the educational activity in their Bureau Notes.

October 12

A "Stop. Think. Connect." (stopthinkconnect.org) flyer was distributed via email blast to staff announcing a one-hour Cyber Workshop scheduled for Friday, October 30, at 9:30 a.m. in the Port Board Room. Those attending were asked to R.S.V.P. Employees could also participate online.

October 30

A total of 80 employees participated in the workshop.

The guest speaker was FBI special agent Todd Munoz, who focuses on cyber security for the Bureau, and his topic was "Keeping yourself safe..." He shared ways to stay safe online and described actual cyber incidents seen by the FBI. A lively question-and-answer session followed.

During a "Trick-for-a-Treat Exchange" at the end of the month, participants were asked to turn in the USB flash drives they had received on October 9 in exchange for a cyber security coffee mug filled with candy.

Port of LONG BEACH
The Green Port

2015 AAPA Communications Awards

Classification: Promotional/Advocacy Materials

Title: Cyber Security Employee Training

The only expenses were the cost of the USB flash drives ($2,000) and the candy-filled coffee mugs ($3,430), exceeding the original budget of $5,000 by $430. Information Management and Communications invested a total of 150 staff hours.

5. Communications Outcomes and Evaluation Methods

This National Cyber Security Awareness Month activity increased interest and awareness of the Port's Cyber Security Program and also helped the Port's nearly 500 employees learn how to take advantage of the cyber security services available from the Information Management Service Desk.

During the educational activity, after receiving the tricky USB drive, it was clear that employees need to be more careful:

- 17 individuals called the Information Management Service Desk or other Information Management staff to notify them about this "threat" and received kudos for being alert to potential cyber security issues.
- 108 individuals plugged it in, reaching the "cyber gotcha page."
- 32 individuals filled out an external form requesting potentially sensitive information.
- The cyber-expert speaker was very well received and shared valuable information with:
- 80 employees attended the speaker presentatation in person or online.
- At the "Trick-for-a-Treat" location where staff turned in the flash drives:
- 468 individuals made the exchange for cyber security coffee mugs filled with candy.