



Message from the President
DeBorah Lozada, Ph.D., CBCP

2006 Theme:

We want to continue an environment involving the exchange of experience and information. Our theme for 2006 is ***'Work Smarter, Partner Harder'***.

The Orange County Chapter has made significant strides in the number and types of professional development activities that it offers to our members. Just a few years ago, the main professional development activity and networking event was the monthly luncheon meeting and the main communications to members was the quarterly newsletter.

Since that time, we have concentrated on enhancing professional development and communications to our membership to meet the growing needs of a diverse and growing chapter. In 2006 we will continue to strive to provide quality topics and speakers as well as special events to increase our visibility within our industry and communities. The Board has been active in preparing our monthly meetings and scheduling weekly and quarterly communications to our members. Taking a quick look at our current chapter calendar, the following events are scheduled:

- Monthly luncheon meetings with topics specific to industry needs
- 22nd Annual Disaster Recovery Alliance (DRA), on May 10.
- Sponsorship of the July DRII Certification course and exam

In addition:

- Distribution of the weekly eNews blasts with important dates and topics, such as voting on the new bylaws which occurred on March 3rd.
- ACP-OC Website which was enhanced in 2005 and will continue to be a source of information to members and non-members.
- ACP Corporate continues to enhance communications to the chapter presidents and members.

We will expand our monthly meetings to include topics that help our members, industry and communities in both disaster and business recovery management.

As professionals, we are constantly using our skills in developing plans; maintaining/monitoring plan updates; facilitating plan exercises; managing

budgets; conducting risk assessments and business impact analyses; and managing incidents. As business leaders we need to mentor, communicate effectively, and provide the inspiration and momentum to sustain the business continuity or disaster recovery program. You will see future ACP-OC events addressing these areas such as "Emergency Management in Orange County" and "Managing Information in Complex Environments: Understanding Signals-Preempting Crisis".

Another area we will pursue is greater visibility within our industry and communities by contacting the Chambers of Commerce within our areas to offer our services to mid and small businesses. Last month the Chapter leadership initiated communications with the Fountain Valley, Huntington Beach and Costa Mesa Chambers of Commerce. Watch for future activities and volunteer opportunities to partner with mid and small businesses within our communities on business continuity planning.

ACP-OC is working diligently to continue delivering programs and events that further your professional growth and provide an exchange of experience and information.

Although I have met many of you at different meetings and seminars, there are a few whom I have not had the opportunity to meet. Please drop me an e-mail or introduce yourself at one of our monthly meetings. I look forward to meeting you.

DeBorah Lozada, Ph.D., CBCP
ACP-OC President
DeBorahLozada@aol.com

INSIDE THIS ISSUE

Message from the President	1
Upcoming Events	2
Basic Facility Security	2
New Members	2
Article #1 –Basic Questions to answer about Business Continuity	4
Chapter News	5
Article #2Emerging Internet Threats for 2006	6
ACP Bylaws	8
Monthly ACP Survey Report	12
Executive Board	14



UPCOMING EVENTS

ACP CHAPTER MEETINGS Orange County

Time: 12:00 p.m. – 3:00 p.m., Capital Group Brea, CA

- 04/12/06: "Rapid Continuity", presented by Phil Lambert, Center for Continuity Leadership
- 05/10/06: **No Chapter Meeting**
(See Events Section)
- 06/14/06: "2005 Trends in the BC/DR Market and Salary Survey Results", presented by Cheyenne Hasse, President, BC Management, Inc.
- 07/12/06: **No Chapter Meeting**
(See Events Section)

EVENTS

- 05/10/06: **22nd Annual Disaster Preparedness Academy, Anaheim, California**
Please refer to the website below for conference flyer. All ACP Members can get a non-profit discount
<http://www.oc-redcross.org/show.aspx?mi=3205>
- 07/12/06: **2nd ACP-OC Hosted DRIL Course and Exam**
Please refer to the website below for additional information.
<http://www.acpoc.com>

CONFERENCES/SEMINARS

- 05/08-05/10/06: [Continuity Insights Management Conference, New Orleans, Louisiana](#)
- 05/23-05/25/06: [CPM 2006 WEST, Las Vegas, Nevada](#)
- 04/01-08/30/06: [Homeland Defense Journal Training Conference™, Arlington, Virginia](#)
Please refer to the website below for additional information:
market.access@verizon.net



Want to advertise your company, seminar, or would like to submit a Newsletter article?

Contact: Stephanie Minasian, Advertising Director
SMinasian@acpoc.com

Contact: Russ Arnett, Newsletter Director
rarnett@acpoc.com

Basic Facility Security

Joe Arnett, M.B.A.

One important aspect of business continuity planning is risk mitigation. Here are some tips for maintaining secured facilities.

Doors and Locks

- Locks should be on all doors, desks and file cabinets. Keep doors locked at all times to unattended rooms with computers and equipment such as phone closets, communications gear, etc.
- Consider cipher locks or access cards for frequent traffic into areas that house your important information.
- Anonymity - do not use signs such as "Server Room" on doors
- Alarms
- Floor-to-ceiling walls around these sensitive areas

Secure Software

- Store securely and lock away all software disks, backup disks and tapes
- Isolate sensitive data such as payroll, financial, or systems with very sensitive data from both the internal network and the Internet
- Monitor dial-in modems. Be aware of direct modem dial-in connections to a computer. Many computers have them and can answer calls made to them
- Separate computers physically
- Consider hardware and data theft prevention devices:
 - Install Removable hard drives - locked away at night
 - Use tie-down cable locks for laptop and desktop systems

Inventory

- It is important to know what you have. Confer with your insurance agent on the best way to document and update your inventory and keep a copy of the inventory off-site.



VENDOR ADVERTISEMENT

Simpler Life's

Since 1981

**NEWLY
STRENGTHENED!**

Deluxe "Shelter in Place" 5 & 10 Person 72 Hour Disaster Kits

- Ideal for any Facility • Three packaging choices • Good for Evacuations too!
- Custom built Kits available for your Climate & Risks...
Hurricanes, Snow, Tornados, Floods, Earthquakes.

	5 Person	10 Person
Food		
S.O.S. Food Bars (5-yr. shelf life, 3600 Calories)	5	10
Water		
Water Pouches 4 oz. (5-yr. shelf life)	48	96
Bottle of Water Purification Tablets (50)	1	1
Warmth		
Emergency Blankets	5	10
Personal Safety		
Work Gloves	1	2
Dust Masks - N95	5	10
Lighting		
12 Hr. Green Light Sticks	1	2
30 min. Yellow Light Sticks	1	2
Flashlights	1	2
"D" Cell Batteries, Alkaline	2	4
Support		
Box of Waterproof Matches (50)	1	1
Multifunction Tool	1	1
Pry Bar 18"	1	1
Tarps 8' x 6'	1	2
Nylon Cord 50'	1	2
Duct Tape 2" x 50 yds.	1	2
Survival Bag - for Waste, Body Bags, Sealing Windows, etc...	1	2
Medical Heavy Duty Kits w/ QuikClot		
2 Patient Deluxe Kit	1	---
5 Patient Deluxe Kit	---	1
Hygiene/Comfort/Sanitation		
Refreshing Large Wipes (8 pk.)	2	4
Toilet Seat Covers (5 pk.)	3	6
"Wag" Sanitation Bags - Jells Liquids, up to 60 oz., Process solids...	5	10
Personal Hygiene Kits in Ziplock		
Each Kit Contains:		
15 - Moist Towelettes		
1 - Tissue, Pocket Packs		
1 - Comb		
1 - Toothbrush		
1 - Toothpaste		
Communication/ Instruction		
Survival Guides	1	1
Whistle w/ Lanyard	1	2
Solar Crank Radios - (No Batteries Req.)	1	1
Packaging		
Choice of Duffles, Rigid Industrial Tote & Mobile Kits		



5 Person Duffle Kit shown

NEW
QuikClot with both medical kits
QuikClot stops bleeding almost instantly!

5 Patient Medical Kit Contents
(See-through waterproof pouch)

1 - QuikClot	2 - Coldpacks
3 - ABD Pads (5" x 9")	2 - Triangular Bandage
12 - Gauze Pads (4" x 4")	3 - Safety Pins
6 - Butterfly Closures	4 - Sugar Pack
2 - Gauze Roll (2" x 5 yds.)	1 - 2" Elastic Bandage
2 - Gauze Roll (3" x 5 yds.)	8 - Antiseptic Wipes
1 - Eye Pad	8 - Antibiotic Ointment
1 - Shock Blankets	1 - EMT Scissor
8 - Q-Tips	1 - First Aid Guide
1 - Splints/Tongue Depressors	10 - Exam Gloves
4 - XL Band-aids	1 - Forcep / Tweezer
10 - Band-aids	1 - Penlight
1 - 1" Tape	

- 5 Person Duffle Kit # 0106080D \$219.00
- 5 Person Tote Kit # 0106080T \$219.00
- 5 Person Mobile Kit # 0106080M \$289.00

- 10 Person Duffle Kit # 0106081D \$329.00
- 10 Person Tote Kit # 0106081T \$329.00
- 10 Person Mobile Kit # 0106083 \$399.00

High Strength Industrial Totes with
Tamper Resistant Ties & Adhesive Signs
• (5 Person) Tote size: 21.5" L x 15.5" W x 12.5" H
• (10 Person) Tote size: 21.5" L x 15.5" W x 17" H



Simpler Life Emergency Provisions, Inc.

2035 Park Ave. Suite #1
Redlands, Ca. 92373

www.simplerlife.com
1-800-266-PREP (7737)

P.O. Box 700704
San Jose, Ca. 95170

(909) 798-8108 • Fax (909) 798-8718

(408) 973-1222 • Fax (408) 973-0470



Basic Questions About Business Continuity

Russ Arnett M.B.A., MBCI, CBCP, PMP

In preparing for the review, audit and/or development of a Business Impact Analysis, (BIA), over the years I've compiled the following critical questions that have help in streamlining the process and ensuring that I capture the necessary data to complete a BIA.

Information Security

1. When was the last time you experienced a breach of security that resulted in damage to valuable company information?
2. How do you currently ensure the confidentiality, integrity, and availability of your firm's critical data and information technology?
3. How do you protect your communications networks from unauthorized internal or external access?
4. How do you protect the information being communicated among your staff and external users?
5. How do you identify and validate potential threats to your information systems and networks?
6. How do you identify and validate potential vulnerabilities to information systems and networks?
7. How do you protect your employees from identity theft?
8. What policies and procedures have you established for dealing with data protection and network security?
9. How do you measure the effectiveness of the security programs you have in place?
10. How often do you test your information security programs, and when was your last test?

Physical Security

1. When was the last time you experienced a security breach that allowed someone's unauthorized access to your offices?
2. What was the outcome of that occurrence?
3. How do you currently control access to your properties for employees and guests?
4. How do you identify potential security threats within your premises?
5. How do you identify potential security threats external to your premises?
6. How do you monitor your corporate property's perimeters?
7. How do you currently respond to existing security threats?
8. What policies and procedures have you established to protect your physical premises from unauthorized access?
9. How do you measure the effectiveness of the physical security programs currently in place?
10. How often do you test your physical security programs, and when was your last test?

Special Thanks Volunteers Newsletter Committee

Christian Lozada - Technical Writer and Reviewer

John Winn – Journalist

If you would like to join the Newsletter Committee please contact Russ Arnett, Newsletter Director, rarnett@acpoc.com

THANK YOU



21st Century Software, HP,
MissionMode Solutions, and Agami
Systems for sponsoring our January,
and February and March and April
Chapter meetings



Basic Questions to answer about Business Continuity: (continued)

Business Continuity

1. What are your most critical business processes and supporting systems (e.g., payroll, A/P, manufacturing)?
2. If those processes and systems were no longer available, how would you get yourself back into business?
3. How do you currently minimize the damage to your business from disabled or compromised information systems?
4. What procedures do you initiate to recover systems and processes that have been disabled or destroyed?
5. How will your employees respond in an emergency situation, especially one that involves evacuating the premises?
6. If you were no longer able to access your office, for whatever reason, how would you restore business operations?
7. Facing a disaster situation, how would you notify employees, family members, local authorities, and clients?
8. What policies and procedures have you established to keep your company in business following a crisis or disaster?
9. How do you measure the effectiveness of these response, recovery and restoration programs?
10. How often do you test your business response and recovery programs, and when was your last test?

Emergency Management

1. When was the last time you experienced a crisis or disaster situation that threatened your business, your employees or your family?
2. What was the outcome of that event?
3. How do you currently respond to emergencies and other crisis situations?
4. What procedures are in place to mitigate the severity or outcome of potential disasters?
5. How would you describe your company's level of preparedness for dealing with crisis situations?
6. What is your normal level of interaction with public authorities, such as police/fire/EMT, and city/county/state offices of emergency management?
7. Faced with an emergency, how would you interact with those same public sector organizations?
8. What policies and procedures have you established to deal with emergency situations?
9. How do you measure the overall effectiveness of existing emergency and crisis response programs?
10. How often do you test your emergency and crisis response plans, and when was your last test?

BUSINESS CONTINUITY PROFESSIONALS WANTED

California State University, Fullerton is looking for Business Continuity Professionals to join an advisory board.

Date: May 18, 2006 **Time:** 11:30a.m. – 2:30p.m. **Place:** CSUF Campus

If you are interested in exploring the educational feasibility of developing a Business Continuity Certificate Program at CSUF, please email DeborahLozada@aol.com.





Emerging Internet Threats for 2006

Russ Arnett M.B.A., MBCI, CBCP, PMP

As professionals, we should be the ones that are pushing our organizations to keep up-to-date on threats and how to mitigate against them.

- **Hackers Use Instant Messaging To Spread Viruses and Worms:** In 2005, use of Instant Messaging and text messaging services in the home and at the workplace continued to increase. In conjunction with social engineering tactics, hackers and criminals are starting to exploit IM services, to infect computers with viruses and worms. Even though IM and text messaging attacks are not yet commonplace, a few new IM viruses like the “Virkel Instant Message Virus” were unleashed in 2005. The Virkel virus opened a backdoor in consumers’ security software, giving hackers access to files and personal information and disabling parts of anti-virus and other security software. Since consumers are largely unaware of the fact that IM and text message services can be used to spread viruses, they are extremely vulnerable to these types of attacks.
- **Phishing Fraud Becomes More Prevalent and Sophisticated:** By the end of 2005, phishers had started to shift their tactics from large scale e-mail blitzes to more targeted and concentrated attempts. One example of such a targeted approach is called “spear phishing.” This form of phishing email targets a group of people within a specific company or organization, often appearing to be sent from an internal employee in the human relations department, IT department or even a former colleague. This tactic can be more effective than a generic phishing attempt, because “spear phishing” emails may look and feel just like emails employees are used to getting regularly from their company or organization. Spear phishing banks on the fact that recipients won’t question the legitimacy of the emails.
- **Viruses Attack Cell Phones and PDAs:** Mobile wireless devices, like cell phones and PDAs, are becoming increasingly vulnerable to hackers and viruses. Last year, the number of viruses and worms that affected cell phones and PDAs increased substantially. Mobile device viruses like “Cabir” and CommWarrior.A,” could read addresses and phone numbers and spread from mobile phones and BlackBerrys through Bluetooth connections and mobile messaging services without the user’s knowledge. While these types of attacks have not become pervasive, they have the potential to infect and spread from devices consumers least expect and target devices that probably lack security protections.
- **Hackers Target Online Brokerage Accounts:** In 2005, there were increased reports of hackers using malicious code to crack consumers’ online brokerage accounts. Hackers exploited vulnerabilities in consumers’ computer security to steal passwords and brokerage account information. They used the stolen information to sell the unsuspecting consumer’s stock and then transfer the proceeds to an online bank account, where it was withdrawn. Since the nature of online brokerage accounts makes it easy to transfer funds from various accounts outside the firm, online brokerage accounts are attractive targets for hackers and thieves.
- **Internet Crimes Go Unreported:** Although the number of Internet crime victims rose in 2005, those victims rarely filed a report with the FTC or notified a police department of the crime. According to the Federal Trade Commission’s “2005 Consumer Fraud and Identity Theft Complaint Data,” 61% of Internet fraud victims did not notify law enforcement when victimized by Internet crime. Moreover, the FBI’s “2005 Small Business Computer Crime Survey” indicated that only 9% of those businesses that experienced a computer security incident reported it to a law enforcement agency. Not reporting crimes to law enforcement makes it more difficult to catch and prosecute online criminals, allowing them to operate with impunity.



Member Spotlight – April 2006
William Walker
First American Corporate

William’s current role is to develop and document Disaster Recovery Plans for CITG/PISG within the First American Corp. in Santa Ana, CA.



VENDOR ADVERTISEMENT



Bringing Intelligence to Backup and Recovery

No matter how well managed your IT center may be ...

There will be times when reliable backups are needed to recover vital corporate data. It might be due to a power blackout, or weather related. It could be the result of a virus infection, or even a malicious act. Or it may simply be a common processing problem, or just human error.

Whatever the cause, your backup is your protection, your means of recovery. 21st Century Software provides the only truly automated, intelligent enterprise solution for backup and recovery management.

Take a moment to learn how your organization can benefit from our VFI Product Family.



ACP Bylaws:

On January 7, 2006, the ACP Corporate Board of Directors approved new bylaws for the organization. The 2006 chapter presidents were also given an opportunity to review the document and provide their feedback.

The ACP Corporate Board is pleased to announce the following highlights to the bylaws:

- Adding “continuity of operations” as one of ACP’s professional purposes
- Removing the restrictions on lobbying activities (BCP-related legislation only)
- Enabling the Corporate Board to modify the Code of Ethics statement and document
- Reclassifying the categories of membership to include:
 - General Individual Members
 - Chapter Individual Members
 - General Organizational Members
 - Chapter Organizational Members
 - General Affiliate Members
 - Student Members
 - Honorary Members

VISIT OUR WEBSITE
<http://acpoc.com>



- Adding provisions to increase the Corporate Board from 8 to 12 as the membership and the number of chapters continue to expand
- Expanding Corporate Board eligibility to include Chapter directors who have two years of chapter board experience
- Adding a consecutive term limit of four years for the Chairman, Recording Secretary and Treasurer positions

The ACP Corporate Board brought the document to the membership for their review and approval on March 3, 2006. The new bylaws passed 96% to 4%.

The Corporate Board will provide additional details on the implementation of the approved bylaws as they become available.

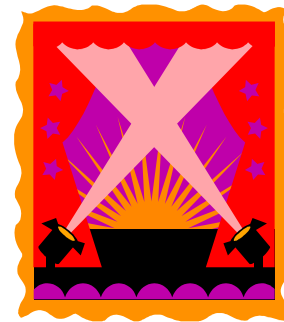
I would like to take this opportunity to say a big **"thank you"** to all those who voted. Your support and enthusiasm will enable us to achieve great things in 2006.

Sincerely,
DeBorah Lozada, Ph.D., CBCP
ACP-OC President
DeBorahlozada@aol.com

Welcome Returning ACP Members

Rick Iverson
DeBorah Lozada
Donovan Lozada

DCC USA
UnitedHealth Group
RxSolutions





Pandemic Planning

Russ Arnett M.B.A., MBCI, CBCP, PMP

How Influenza Spreads

The primary route that influenza virus is spread is through direct contact, or touching commonly used contaminated surfaces such as door handles, and then transferring the virus by touching your eyes, mouth or nose. Droplets from an infected person can also travel through the air from sneezes and coughing and reach the eyes, mouth or nose. With a little thought, it is easy to see how normal behavior makes it easy for the virus to be transmitted. Some examples of normal and dangerous behavior during a pandemic are listed below.

Important Fact:

Influenza flu virus can remain infectious for:

- 48 hours on a non-porous surface
- 8 hours on a porous surface such as clothing or furniture
- 5 minutes on your hands

Good hand washing and hygiene practices are the most important steps for minimizing exposure to influenza infections. Wearing gloves, the right mask and goggles are effective barriers. Placing these barriers between your nose, mouth and eyes are important when venturing into areas potentially contaminated with infectious particles secreted through coughing and sneezing as well as transferred through hand to mouth contact.

General Measures to Protect Yourself and Your Family

Pre-pandemic recommendations:

- Everyone should be immunized with the up-to-date Influenza vaccine
- Stay home when you are sick.
- Follow safe practices at home or in public when you are sick
- Have a contingency plan for essential supplies at home
- Maintain good hand hygiene
- Clean/disinfect surfaces in your environment
- Educate family members, especially children, in personal hygiene
- Use protective personal equipment when providing direct care to a sick person

Preparing For the Pandemic

There is no ability to predict the reaction of the public once the World Health Organization, CDC, Health Canada or the news media announces the sudden emergence of a pandemic. This news may cause widespread panic, hoarding of essential goods and medicines, shortages of essential goods, service interruptions including supply of electricity and water, and a major economic slowdown that will have financial implications for everyone. Being prepared ahead of time is essential to reduce the impact of the pandemic on your family and on the economy.

The global economy has been developed around a just-in-time inventory strategy. For example, most municipal water treatment facilities maintain a 5 day supply of chlorine to treat drinking water. An interruption in any link in the manufacturing or transportation of chlorine could shut down the water supply system. These seemingly impervious systems are delicately linked and will be prone to interruptions.



Pandemic Planning-Continued

Once a pandemic has been declared, sourcing essentials will become very difficult. Therefore, now is the time to purchase adequate supplies. Plan to keep a 2-3 month supply of essential items to sustain your family. Rationing will be required.

You should have bottled water stockpiled in case municipal water supply interruptions occur. Plan for 2 liters of water per person per day. To cover a two-month period, you will need 120 liters per person. Buying water in bulk containers is the most cost effective. Stockpiling canned juices should be also be considered.

Consider canned foods, dry foods and powdered milk to be used with dry food like cereal. Consider how much each person in your family eats in a day and multiply by 120 to get a minimum supply of these foodstuffs.

Fresh fruits and vegetables will not be available unless you can grow them in your own yard (a

good idea). Frozen fruits and vegetables may be practical but there is no guarantee electricity will be maintained so refrigeration may not be a good strategy. Maintain a 2-month supply of multivitamins for each person in your family.

There may be substantial interruptions in the ability to heat your house or apartment due to potential interruptions in natural gas and electricity supply for extended periods of time. Consider keeping propane canisters/cylinders for your BBQ, a good supply of naphtha for camping stoves/heaters and candles for local heating. Batteries and flashlights are also a good idea. Keep fully functioning carbon monoxide detection devices in your home at all times in spaces where portable cooking devices are used.

Maintain a supply of other essentials that may be particular to your families needs. These would include diapers, specific medicines, general medicines such as aspirin, acetaminophen, other over the counter medicines (not necessarily for flu symptoms) etc.

Entertainment will be difficult in prolonged periods of an outbreak. This may seem trivial but with children, it is essential. Collect a large variety of books, games, videos, etc as travel into the community will be reduced or eliminated.

During a Pandemic Outbreak

Eliminate all group activities including:

- Daycare
- School
- Church
- Sporting and entertainment activities
- Public transit

Do as much activity from home as possible including:

- Internet banking
- Working from home (assuming your employer has work)
- Communication with friends and family should be by phone or email
- Outside travel into the community should be done by as few people as possible. Travel as a family should be minimized.
- Limit essential activities only to people you are very confident have not been in contact with infected people.

Minimize or eliminate all outside/in-public activities to those that are essential such as:



Pandemic Planning-Continued

- Necessary doctors visits (delay these until the pandemic passes if possible)
- Essential shopping
- Phone first to confirm availability of required items if possible
- Always wear the N-100 mask, goggles, appropriate gloves and use hand sanitizers or wipes when out in public. The mask can be reused after 72 hours.
- Never touch your face without sanitizing your hands first.
- When returning home, “decontaminate” yourself before interacting with other family members.
- Disinfect reusable gloves with a household bleach solution. A 100ppm solution is an effective sanitizer or mix household bleach 1 tsp. in 1 liter (or 1 quart) of water
- Shower and wash clothing
- Do not wear shoes in the house that you have worn outside the home in potentially contaminated areas such as shopping centers.
- After handling money, packaging (such as a grocery box or bag) or any surface such as a grocery cart, public phone, gas pump handle, key pad etc, always wash or sanitize your hands.

Below are examples of day- to-day high-risk behavior and steps you can take to mitigate your risk of infection. In the time of pandemic outbreaks, eliminate or minimize these activities as much as possible. If you must, use gloves and/or sanitizing wipes on all contact surfaces.

Going to the Library

Most libraries have computers available for the public to access the Internet. Library patrons cough and sneeze over the keyboards, books, DVD's etc. all day long. You must assume the contact surfaces are contaminated.

Use of Shared Computers, Telephones etc.

Any computers, telephones and keypads which are shared are a source of germs.

Wear gloves and decontaminate them with alcohol or chlorine bleach after each use.

Handling Money

Money changes hands every day in stores and banks. We all know that cashiers and bank tellers are not washing their hands every time they handle money and neither are the individuals using their services.

When handling money, wash hands before touching your face, etc, and especially before eating. Glove use during pandemic outbreaks is highly recommended when handling money.

Public Equipment Such as Debit/Credit Card Keypads, Phones, Computers, Video Games etc.

These types of equipment are coughed and sneezed over and handled daily by all sorts of people. They are rarely, if ever, disinfected. Minimize or eliminate their use. If you must use them, disinfect where possible and use gloves. In restaurants, especially fast food, people often use debit cards and touch the key pad to pay. Minimally, cash is handled before you eat, and you often eat with your hands.

Wash hands before eating in these environments at all times.



Pandemic Planning-Continued

Full Serve Gas Stations

On cold days we sometimes go to the full serve gas station and pay by credit card. The attendants work outside and sometimes are ill, coughing and wiping their noses with their gloves. They hand you the pen and clip board to sign your credit card slip. Then off we go to dinner.

In these situations, always have your own pen. If you handle the clipboard, use gloves. Wash hands before touching food or other people.

Grocery Cart Use

Children are drooling on the handle or wiping their hands on their nose and then holding the handle. The handle may be contaminated and can contaminate you or your child.

Before you put your child in the cart, sanitize the surfaces with appropriate wipes or spray.

Pets

Pets walk in the fecal matter of other animals (birds as well). The virus can live in fecal matter. Monitor your pet's activities closely.

Monthly ACP-Orange County Chapter Meetings Survey Results

January 2006

- "Selecting the Best Recovery Site?", presented by Rich Schiesser, RWS Enterprises
 - "Program Development for Enterprise BC & Testing", presented by Ed Sullivan, Gemstar – TV Guide
- 90% rated the presentations favorably.

February 2006

- "HP's Business Continuity Services Overview", Mark Garner (ABCP), BCS Client Principal, HP HP Business Continuity Services
- "Office Recovery - Bringing the People to the Recovery", John Pagliaro, Solution Design Manager, HP Business Continuity Services

78% rated the presentations favorably.

March 2006

- "Emergency Preparedness in Orange County" presented by Dona Boston, Orange County Sheriffs Department, Emergency Management Bureau

93% rated the presentation favorably.





VENDOR ADVERTISEMENT

3 Business Continuity Workshops Coming To California ACP Members To Receive Discounts Up to \$130

**Essentials for Enterprise-Wide
Business Continuity
Programs**

**How to Benchmark and
Sustain Your Program**

**How to Create Drills and
Exercises... *That Work!***

Workshop #105: Essentials for Enterprise-Wide Business Continuity Programs

Attendees learn best practices for designing and implementing a comprehensive, properly sequenced, enterprise-wide Business Continuity Program. All elements of disaster response and business recovery are covered, including examples collected from 17 years of successful planning with organizations such as Toyota, Macy's, California Public Employees Retirement System, Discovery Communications, Yamaha, and many more. Content is appropriate for any experience level, but it is especially geared for beginning business continuity managers and executives from various departments who oversee such programs. DRII-certified professionals who attend this session can receive 4 continuing education points for re-certification. Half day. \$195 per seat. ACP members pay only \$165.

Workshop #201: How to Benchmark and Sustain Your Program

This session examines emerging standards and best practices for keeping a program current and extending its reach. Standards include NFPA 1600 for organizing and administering your program and the Incident Command System for improving crisis communications. Using these standards, attendees examine best practices for continuous program improvement, creating more mature action plans, and improving logistics and facilities. DRII-certified professionals who attend this session can receive 8 continuing education points for re-certification. One day. \$395 per seat. ACP members pay only \$345.

Workshop #301: How to Create Drills and Exercises... *That Work!*

Participants review best practices for designing and implementing effective drills and exercises for a business continuity program. You will study proven steps for constructing exercises efficiently, using industry best practices. You will examine examples of 4 types of exercises, including an orientation session for executives, a communications drill for an IT department, and a table-top exercise for a business unit. Then you will participate in designing and executing a functional exercise for an Emergency Operations Center. DRII-certified professionals who attend this session can receive 8 continuing education points for re-certification. One day. \$395 per seat. ACP members pay only \$345.

These workshops are sponsored by Disaster Survival Planning Network (DSPN). They are professionally designed to be educationally sound. Instructors employ lecture, video clips, and breakout exercises to deliver an energetic, content-rich agenda that is thought-provoking as well as entertaining. Each participant receives a ring binder detailing the proceedings and providing additional reference materials.

Content for these workshops was developed by Judy Bell, a former Division Manager for Pacific Bell, and author of the first book on business continuity for the private sector, [Disaster Survival Planning: A Practical Guide for Businesses](#). She is a frequent speaker at national and international conferences.

Visit this link for more details and to register online: www.disaster-survival.com/workshop.html

To receive your ACP discount, register using this promotional code: "ACP 2006"



How to Reach our Executive Board

President

DeBorah J. Lozada
PacifiCare
(714) 226-2683
dlozada@acpoc.com

Vice President

Bill Wostenberg
Automobile Club Southern of California
(714) 885-1534
bwostenberg@acpoc.com

Secretary

Lynn Manzano
Experian
LManzano@acpoc.com

Treasurer

Susan Zielan
Experian
(714) 830-7115
susan.zielan@experian.com

Information Director

Kern Vogel
kvogel@acpoc.com

Newsletter Director

Russ Arnett
Molina Healthcare
(562) 951-1531
rarnett@acpoc.com

Program Manager

Alicia Stevens
BC Management
(949) 250-8172 ext.203
astevens@acpoc.com

Website Director

Tym Stark
The Aerospace Corp.
(310) 336-6857
tstark@acpoc.com

Resource Director

Susan Jacobo
Southern California Edison
(626) 302-7012
sjacobosk@acpoc.com

Membership Director

Sandy Rheinecker, WFS Financial
949.743.3963
SRheinecker@acpoc.com

Advertising Director

Stephanie Minasian
Iron Mountain
SMinasian@acpoc.com

Former President

Monique Weiland
California ISO
(626) 537-2712
mweiland@acpoc.com

Service Project Chair

Open Position

Welcome New Members First Quarter 2006



- | | |
|----------------------|---------------------------|
| Brent Comfort | SunGard |
| James Harris | US Marines |
| Chris Sloper | Experian |
| Zachary Michelson | OCHCA |
| William Walker | First American Corp |
| Joseph Wintering | N/A |
| Craig Lanier | N/A |
| Jens Hudson | First American Trust |
| Katherine Mary Evans | N/A |
| Diane Coles | Scan |
| Norm Koehler | IMPAC |
| Nana Richardson | Data Corp |
| Daveeda Mason | CC Capital Holdings |
| Peter Benett | Alchemy Communications |
| Irene Long | OCTFCU |
| Jess Chacon | Toyota Motors |
| Philip Bigge | Countryside Financial |
| Rick Range | ACS/County of Orange |
| James Euopulos | Sullivan Curt's Monroe |
| Stacy Hudson | Fremont Investment & Loan |