Crist Wagner, RSSP
President/Programs
Keystone Law & Justice
714-539-3495
omercrist@aol.com

Jim Weidner, RSSP
President Elect
Basic Safety Services
626-523-6053
jjweidner@ca.rr.com

Violet Pisani
Secretary
CAL/OSHA Consultation
818- 901-5121
vp@hq.dir.ca.gov

John A. O'Toole, RSSP, FIAE
Treasurer/Membership
General Safety Services
323-258-2771
otoole47@adelphia.net

Peter Gin, RSSP, FIAE
Newsletter
Lockton Insurance Brokers
213-689-4203
petergin@earthlink.net

Joann Blayney, RSSP
Public Relations
Safety Dynamics Group
562-981-5335
joannb8041@aol.com

October 5, 2007 Lunch Meeting

12 Noon

California State University, Dominguez Hills
Extended Education Building
1000 E. Victoria Street
Carson, California 90747

Mandatory Confirmation w/John O'Toole
By 10/2/07 @ (323) 258 – 2771

Linda Hunter, RSSP, FIAE
Webmaster
Zee Medical
714-847-8852 ext 234
lhsafenet@aol.com

Vincent J. Takas, RSSP, FIAE
Nominations/Awards
The Walt Disney Company
818-553-4318
vincent.j.takas@disney.com

Charles A. Merriam, RSSP
Sgt. at Arms
Reaching Higher Risk Management
909-738-0651

Scott Mackay
University Liaison
CSUDH
310-243-2425
smackay@csudh.edu

Joseph M. Kaplan
Corporate Scholarships
President Emeritus, NSC
310-652-1932

Byron Jamerson, RSSP, FIAE
CSSSP Training Institute
323-258-2771
jammo70@hotmail.com

Andrew Asaro
Scholarship Raffle Chair
562-864-9755

Dan Leiner
Vice President/Placement
Cal/OSHA Consultation
818-901-5755
dleiner@hq.dir.ca.gov

CSSSP – Los Ángeles Chapter
2272 Colorado Blvd. Ste. 1368
Los Angeles, CA 90041
(323) 258 – 2771
www.csssp.com

C S S S P

California Society of Safety & Security Professionals
Los Angeles County Chapter

Volume 49 October 2007

October Speaker

Ms. Astra C. Townley, MS, ARM, CSP, with Liberty Mutual Insurance Company, provides safety consulting and training services to national market loss prevention clients throughout the Pacific region. She assists in the development and implementation of occupational health, ergonomics and disability management. She will discuss how risk management interfaces and supports the health, safety and security professions. Join us for a most informative presentation.

August Speaker

Dr. Denise Herz, Ph.D. provided an overview on Criminal Justice, Security and Safety in their shared realities and provided examples of how these fields must communicate and collaborate to reach their commonly held goals of improving the public safety and the well-being of the communities.

Memberships

Wanda Kay Arns, Student Member
Osiris Y. Ayoola, Student Member
Mario Manriquez, Student Member
Jared G. Williamson, Student Member
William J. Jones, Professional Member
John Quagliani, Professional Member
Astra C. Townley, Professional Member

SCHOLARSHIP AWARDS

Mario Manriquez	$1,120.00
Larry Steven Bellomo	$1,120.00

REGISTERED SAFETY and SECURITY PROFESSIONAL

Diana N. Cucuk-Brkic

Professional members, who would like to apply for the REGISTERED SAFETY and SECURITY PROFESSIONAL (RSSP) designation, please contact John A. O'Toole, RSSP Chairman for details. c/o: john@generalsafetyservice.com or 323-258-2771.

President's Message

As CSSSP members, we must, if we are going to contribute as first line defenders, anticipate, recognize and appraise loss risks and take actions necessary to reduce, mitigate or eliminate those risks of loss. Regardless of what area of expertise we have, as loss prevention practitioners, we are saddled with the task of collecting information. Without information that is concise and reliable, our efforts are, at best, inadequate. We know and are skilled at asking the right questions (who, what, where, when, how, and why). But, there is always a "but," to be a "Value Added," professional we need to make sure that the answer to these questions are of value to our mission.

I recently took a CPR/First Aid class from Past CSSSP President Linda Hunter and noted the importance of the answers to a series of questions that she asked. These questions exposed to me, a very distinct marriage among the disciplines of our society (Safety, Security and Environmental Health). That being said, I noticed that I have developed a different view of the direction that I now take when conducting a loss prevention investigation. In other words, my mind set was geared to be the way we made inquiries from a police and security perspective. Nothing else seemed relevant.

Over the past three years, I have studied and practiced the other disciplines of our society and I have become acutely aware of how much I was lacking in my limited view of our charge as loss prevention practitioners. I now take an extended view of collecting information. I attribute this change to the exposure that I have received from the California Society of Safety and Security Professionals.

I wish to thank the CSSSP group for providing me with the opportunity to expand my way of thinking.

Think about it.

"It's so easy a cave man can do it"

Crist Wagner, CPP, RSSP, CFE

Avoid Cashier Check Scams

The Office of the Comptroller of the Currency (OCC) issued an advisory recently that provides advice to help consumers avoid becoming victims of scams involving cashier's checks.

In most of these cases, individuals receive a cashier's check and are asked to deposit the check into their account, wait until funds become available and then wire some part of the funds from their account to a third party, often in a foreign country.

Although the amount of a cashier's check quickly becomes "available" for withdrawal by the consumer after the consumer deposits the check, these funds do not belong to the consumer if the check proves to be fraudulent. It may take weeks to discover that a cashier's check is fraudulent. In the meantime, the consumer may have irrevocably wired the funds to a scam artist or otherwise used the funds -- only to find out later, when the fraud is detected -- that the consumer owes the bank the full amount of the cashier's check that had been deposited.

A cashier's check is an instrument issued and sold by a bank, and is a direct obligation of the bank. For decades, cashier's checks have been used as a trusted form of payment to consumers for goods and services. "Cashier's checks serve an important purpose in the financial marketplace, but we are starting to see an increasing number of scams involving these instruments," said Comptroller of the Currency John C. Dugan. "In most cases, consumers can avoid becoming victims by remembering that, if something sounds too good to be true, it probably is. In addition, our advisory provides a number of specific tips about the types of scams we are seeing today."

There are a number of known scams involving cashier's checks, many involving an unexpected windfall. In one, the victim is advised that he has won a foreign lottery and that the proceeds will be sent to him once the taxes or fees are paid. A cashier's check is provided to cover those charges, and the victim is asked to deposit the check, wait until it clears and then wire funds to cover the taxes and fees. In most cases, the wire transfer is directed to an account in a foreign bank.

While it can be very difficult for consumers to know if a cashier's check is fraudulent, here are a number of specific steps consumers can take to protect themselves:

Try to know the people with whom you do business.

When possible, verify information about the buyer from an independent third party such as a telephone directory. Be cautious about accepting checks -- even a cashier's check -- from people that you do not know, especially since it may be difficult to pursue a remedy if the transaction goes wrong.

- When you use the Internet to sell goods or services, consider other options such as escrow services or online payment systems rather than payment by a cashier's check.

- If you do accept a cashier's check for payment, never accept a check for more than your selling price if you are expected to pay the excess to someone else. Ask yourself why the buyer would be willing to trust you, who may be a perfect stranger, with funds that properly belong to a third party.

- A cashier's check is less risky than other types of checks only if the item is genuine. If you can, ask for a cashier's check drawn on a bank with a branch in your area.
- If you want to find out whether a check is genuine, call or visit the bank on which the check is written. That bank will be in a better position to tell you whether the check is one they issued and is genuine.

- Know the difference between funds being available for withdrawal from your account and a check having finally cleared. Your bank may be required by law to make funds available to you even if the check has not yet cleared. However, it could take several weeks to know if the check will clear or not.

Protect Your Identity

Every day, you share personal information about yourself with others. It's so routine that you may not even realize you're doing it. You may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, buy a gift online, call home on your cell phone, schedule a doctor's appointment or apply for a credit card. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address and phone numbers.

It's important to find out what happens to the personal information you and your children provide to companies, marketers and government agencies. These organizations may use your information simply to process your order; to tell you about products, services, or promotions; or to share with others.

And then there are unscrupulous individuals, like identity thieves, who want your information to commit fraud. Identity theft -- the fastest-growing white-collar crime in America -- occurs when someone steals your personal identifying information, like your SSN, birth date or mother's maiden name, to open new charge accounts, order merchandise or borrow money.

Consumers targeted by identity thieves usually don't know they've been victimized. But when the fraudsters fail to pay the bills or repay the loans, collection agencies begin pursuing the consumers to cover debts they didn't even know they had.

The Federal Trade Commission (FTC) encourages you to make sure your transactions -- online and off -- are secure and your personal information is protected. The FTC offers these tips to help you manage your personal information wisely, and to help minimize its misuse.

Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask about company's privacy policy: Will you have a choice about the use of your information; can you choose to have it kept confidential?

- Read the privacy policy on any Web site directed to children. Websites directed to children or that knowingly collect information from kids under 13 must post a notice of their information collection practices.
- Put passwords on your all your accounts, including your credit card account, and your bank and phone accounts. Avoid using easily available information -- like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number -- or obvious choices, like a series of consecutive numbers or your hometown football team.
- Minimize the identification information and the number of cards you carry to what you'll actually need. Don't put all your identifying information in one holder in your purse, briefcase or backpack.
- Keep items with personal information in a safe place. When you discard receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements, expired charge cards, credit offers you get in the mail and mailing labels from magazines, tear or shred them. That will help thwart any identity thief who may pick through your trash or recycling bins to capture your personal information.
- Consider ordering a copy of your credit report from each of the three major credit reporting agencies (CRAs) every year. Make sure it's accurate and includes only those activities you've authorized. CRAs can't charge you more than $9.00 for a copy and in some states; your credit report is free.
- Use a secure browser when shopping online to guard the security of your transactions. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

Secure Laptops, PDAs, Cell Phones

More and more businesses are providing employees with laptops, personal digital assistants (PDAs) and cell phones for speed, convenience and mobility of communication. The benefits can be enormous, particularly for business travelers. So can the security risks, if proper precautions are not taken. Before handing out these high-tech communication tools, the Better Business Bureau advises business to instruct employees how to protect the security of data that is being transmitted or stored. The following guidelines may prove helpful:

- Always keep your laptop, PDA or cell phone within sight, even when at the office. Lock your business cell phone and PDA in a secure location when not in use.
- Keep your portable device within eyesight and easy reach when traveling. Stealing laptops at airports and from trains and restaurants has become a popular data theft technique.
- If at all possible, do not store any sensitive customer or employee data (such as bank account numbers, ATM codes, Social Security numbers and credit/debit card info) on these portable devices.
- If any employee (a salesperson or telecommuter, for instance) needs to take customer data, employee date or other sensitive information off business premises on a laptop, CD, flash drive or other portable device, insist and make certain that the data is encrypted.
- Password-protect access to the laptop, PDA and cell phone. Also make use of passwords to protect Internet access, e-mail, voicemail and address books.
- Turn off the devices when not in use.
- Do not download or accept file downloads from unknown sources.
- Do not share portable communication/organization tools with others.
- Backup all data regularly and keep back-up disks and other back-up materials in a locked, secure area.
- A final word of caution from the BBB: Do not assume that laptops are the only devices that can be hacked into. Criminals can hack into cell phones and steal stored files, contacts and voice mails. Viruses can also significantly disrupt cell phones. Cell phone owners should check with their providers regularly for updates on security features to make certain they have configured their settings for maximum security.