

# OVERLAND SECURITY SERVICES

## Security Briefing

Offices: 1517 Stowell Center Plaza St. L. Mail: PO Box 145 Santa Maria, CA 93456 (805) 925-2216

Lic # PPC – 15268

Bruno J. Zemaitis CII (1917-2004)

First Quarter 2005

Edward J. Zemaitis, Principal

### **SANTA MARIA POLICE DEPARTMENT HOSTS RENTAL PROPERTY OWNERS/MANAGERS GROUP**

Santa Maria Police Department offers informational meetings for rental property owners and managers the third Monday of every other month

These informal meetings include discussions on security-related subjects and information relevant to property management and the law. Meetings are free of charge or obligation and held at 280 E. Newlove Dr. in Santa Maria.

Telephone Penny Simas-Pastore at the SMPD at 928-3781 EXT 304 for more information.

### **OVERLAND OWNER COMPLETES HOMELAND SECURITY TRAINING COURSE**

Edward Zemaitis, owner of Overland Security Services, recently completed a course on Maritime Security at Camp San Luis Obispo, CA. The instruction was provided by the National Interagency Civil-Military Institute (NICI).

The course addressed the challenges in providing security in a maritime environment; arriving and departing ships, docks, harbor facilities, inland waterways and critical infrastructures. Cargo handling systems were reviewed as were physical security aspects unique to maritime applications.

NICI is a function of the State of California and provides instruction in terrorism, disaster relief and mitigation, and a number of other courses for military and civilian authorities. Those in attendance included active duty military personnel, harbormasters and individuals who were responsible for security at several of California's major harbor complexes.

California boasts an extensive coastline and numerous ports and harbors including San Diego, Long Beach, Los Angeles, Oakland, San Francisco and Stockton and a network of inland waterways. In addition, smaller, non commercial harbors such as Avila Beach, Morro Bay, Ventura and Santa Barbara present other, unique, security challenges.

Sen Diane Feinstein, D-CA, recently convened a hearing of the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security to examine ways to prevent terrorist attacks on or through our nation's seaports. She referred to America's maritime industry as the "soft underbelly" of Homeland Defense.

This course of instruction was designed to train those who would "harden" that soft underbelly.

### **HACKING THE COMPUTER HACKERS**

We live in a computer age. Much of our daily routine often revolves around a computer. In office environments, computers are generally networked together, making the information contained in one, available to others, at other sites. This information, and the access that can often be exploited has created a new threat; that of the computer hacker.

The computer hacker accesses a computer from a remote location. The information that is accessed may be of a benign nature, or have serious consequences, if made public, modified or destroyed.

Unethical competitors may pay handsomely to view a copy of a multimillion-dollar proposal; employees, present or past, with an ax to grind with management may cause catastrophic damage to accounts payable or receivable files. Personal, or embarrassing, information may be divulged or compromised.

Recently, Choicepoint, Inc., a national data broker, announced that their systems had been hacked and the credit records of millions of people had been compromised. Kaiser-Permanente then announced a similar attack on their systems; effecting the health records of many thousands of others. Other recent examples include LexisNexis, another data broker. Due to the complexity of computers and systems, this may be the tip of the iceberg. A noted professional responded that, "There is not much you can do, once the unauthorized access is discovered. The damage is done."

Smaller firms, who do not control a major market share of their industry or have access to the financing necessary when a catastrophic loss of data occurs may simply cease to exist. For those companies who did not prepare for such eventualities, they may not be listed in next year's phone book.

Speaking from my own experience and several years ago, Overland started making duplicate back-ups of our computer records. We did not have a comprehensive system to safeguard our computers or data prior to that time, but as we were to discover, it is never too late to start.

Soon after we developed a schedule for multiple backups of all critical data, we suffered a hard drive crash in our, then, only computer. Insofar as our payroll and accounting records were on that computer, we would have been lost if we had not backed up our data daily.

As soon as a new hard drive was installed, we re-installed our accounting software. We then attempted to upload our data from the backup disks. This process is not difficult and should be practiced often.

At that point, we discovered our backup disks were bad and although our accounting software had indicated the backups were successful, the disks were faulty and the computer could not read from the disks. Fortunately, we had duplicated our backups with a Monday-Wednesday-Friday set and in addition, used a different disk set for Tuesday-Thursday-Saturday backups.

This lesson taught us the value of multiple backups and to regularly test the backup program by performing spot checks on personnel and the actual process of creating back ups.

#### **Additional tips for safeguarding company information includes:**

1. Keep all software up-to-date and install patches, as available.
2. Use anti-virus software and anti-spyware programs on every computer, especially so if they are connected on your network. This includes employees personal computers and vendors. Norton or McAfee are two examples of anti-virus programs. Adware and Spybot are two, no cost and effective, examples of spyware that are available.
3. Install firewalls and change security codes from the default settings.
4. Give employees access only to the data they need to perform their job. Develop access control lists and passwords that aren't easy to guess. Combinations of upper and lower case letters and numbers are the best bet.
5. Develop consistent and practical policies on the use of data, the Internet and email; then enforce those policies.
6. Educate employees, executives and vendors who have access to your network on the importance of computer security. Remind them of the importance of data and access control to the network.
7. Insure those without a reason to access computer networks or data are prevented from contact or tampering with your system.
8. Turn off unused computers, terminals, ports and peripherals. Insure older equipment is as protected as newer models.
9. Map critical assets and understand how they are at risk. Develop plans to address their vulnerability.
10. Review computer security on a regular basis, automate it where possible, and review changes made since the last assessment.
11. Back up all data to a secure site. Do not keep your backups with the computer they are associated with. If

a fire destroys the computer, the plastic backup disks sitting on the computer will be gone too.

12. Lastly, make multiple backups, stored in different, secure locations. Three sets with redundancy will insure that you never lose more than one day's records. If the volume of information is such that hourly backups or twice daily backups are prudent, then develop and implement a plan.

#### **KEY CONTROL SYSTEMS**

Before we sign off, we will touch on a few of the main points on the subject of Key Control. They include the following:

- Control and record who is issued keys for business use. Every key issued should be recorded and the person receiving the key is made responsible for the loss of that key.
- Control over who can make copies or duplicates of issued keys. Use of unique locksets or stamping "Do Not Duplicate" on every key.
- A record of every lock in a particular system or business and how many keys have been issued for that particular lock. Marking each key with a unique identifier to identify that particular key and lock.
- The maintenance of a system of issue, record keeping of locksets and keys, loss and replacement of locksets and keys.

Keys are literally, the "keys to the kingdom." Failure to control access by key control will inevitably result in losses to the business owner, whether the loss is discovered or not

A complete article on Key Control Systems will be included in the next quarterly issue of the *Overland Security News Briefing*.

**Overland Security Services** provides the following services. In addition to publication of the *Overland Security News Briefing*, we offer the following services to business and industry on the Central Coast:

- Uniformed Stationary Security Officers
- Mobile Vehicle Patrol
- Employee background checks
- Security Audits for Business and Home
- Courier Services
- Referral to the full range of security related products and services.

About the Publisher: Overland Security Services, LLC has operated on the Central Coast since 1947 and is licensed and bonded to provide security and informational services to business and industry. Bruno J. Zemaitis, the founder, (1917-2004) remained active until shortly before his passing. His son, Edward J. Zemaitis, now operates Overland and serves as the Editor of the OSB. Any questions regarding the contents of the *Security Briefing* may be forwarded to our offices.

Disclaimer: This is not a solicitation or offer. This publication is designed to provide information on the subject matter covered. It is provided at no cost with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. ---  
*From a Declaration of Principles jointly adopted at committee of the American Bar Association and a Committee of Publishers.*

