

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)

Second Quarter 2005

Edward J. Zemaitis, Manager

OVERLAND SECURITY SERVICES OPENS NEW OFFICES.

After 53 years in business in the same location, Overland has moved to new offices in the Travel House Building at 1517 Stowell Center Plaza, Ste L, here in Santa Maria

For those wishing to contact Overland, we have retained our original Post Office Box (145), in Santa Maria and the telephone numbers we have had since the beginning.

The change of location was prompted by the passing of the founder, Bruno J. Zemaitis and the purchase of Overland by his son, Edward. The new facilities offer an excellent environment for business.

Overland held an open house on March 22nd. The Santa Maria Visitors and Convention Center dispatched a number of "Ambassadors" to help with an official Ribbon Cutting and other festivities. They were a very welcome addition to the event.

The event was attended by Overland clients, employees, friends and family.



Overland Manager, Edward Zemaitis, center, surrounded by Overland personnel and the Ambassadors from the Santa Maria Valley Chamber of Commerce and Visitor & Convention Bureau. The ribbon cutting served as the opening event of the Open House.

Also on display were various types of surveillance equipment, including night vision devices, seismic detectors and a polygraph lie detector. A badge and patch collection drew particular attention.

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.

EFFECTIVELY ERASING OLD COMPUTER FILES

Before selling or discarding an old computer, or throwing away a disk or CD, you naturally make sure that you've copied all of the files you need. You've probably also attempted to delete your personal files so that other people aren't able to access them. However, unless you have taken the proper steps to make sure the hard drive, disk, or CD is erased, people may still be able to resurrect those files. Where do deleted files go?

When you delete a file, depending on trash or recycle bin. This "holding area" essentially protects you from yourself—if you accidentally delete a file, you can easily restore it. However, you may have experienced the panic that results from emptying the trash bin prematurely or having a file seem to disappear on its own. The good news is that even though it may be difficult to locate, the file is probably still somewhere on your machine. The bad news is that even though you think you've deleted a file, an attacker or other unauthorized person may be able to retrieve it.

What are the risks?

Think of the information you have saved on your computer. Is there banking or credit card account information? Tax returns? Passwords? Medical or other personal data? Personal photos? Sensitive corporate information? How much would someone be able to find out about you or your company by looking through your computer files?

Depending on what kind of information an attacker can find, he or she may be able to use it maliciously. You may become a victim of identity theft. Another possibility is that the information could be used in a social engineering attack. Attackers may use information they find about you or an organization you're affiliated with to appear to be legitimate and gain access to sensitive data.

Can you erase files by reformatting?

Reformatting your hard drive or CD may superficially delete the files, but the information is still buried somewhere. Unless those areas of the disk are effectively overwritten with new content, it is still possible that knowledgeable attackers may be able to access the information.

How can you be sure that your information is completely erased?

Some people use extreme measures to make sure their information is destroyed, but these measures can be dangerous and may not be completely successful. Your best option is to investigate software programs and hardware devices that claim to erase your hard drive or CD. Even so, these programs and devices have varying levels of effectiveness. When choosing a software program to perform this task, look for the following characteristics:

- **data is written multiple times** - It is important to make sure that not only is the information erased, but new data is written over it. By adding multiple layers of data, the program makes it difficult for an attacker to "peel away" the new layer. Three to seven passes is fairly standard and should be sufficient.
- **use of random data** - Using random data instead of easily identifiable patterns makes it harder for attackers to determine the pattern and discover the original information underneath.
- **use of zeros in the final layer** - Regardless of how many times the program overwrites the data, look for programs that use all zeros in the last layer. This adds an additional level of security.

While many of these programs assume that you want to erase an entire disk, there are programs that give you the option to erase and overwrite individual files.

An effective way to ruin a CD or DVD is to wrap it in a paper towel and shatter it. However, there are also hardware devices that erase CDs or DVDs by destroying their surface. Some of these devices actually shred the media itself, while others puncture the recording surface with a pattern of holes. If you decide to use one of these devices, compare the various features and prices to determine which option best suits your needs.

EFFECTIVE RECORD RETENTION PROGRAMS CAN PREVENT LAWSUITS.

When Robert F. Byrnie was not hired by the town of Cromwell, Connecticut, he filed a lawsuit against the town claiming that he was discriminated against because of his age. It turned out that the prospective employer had failed to keep the application or any other forms relating to the applicant's case. After the case was filed, the municipality also destroyed the written ballots completed by the screening committee concerning the candidate.

The court ruled that the missing application alone would not have created sufficient evidence to infer

discrimination, but that the missing documents, coupled with the destruction of the ballots, was sufficient to allow the applicant to pursue a discrimination claim. As a result of the ruling, Byrnie has the right to take his claims to a jury. Even if the employer prevails, it will have had to expend time and resources on the case.

As this case (*Byrnie v. Town of Cromwell, 2001*) illustrates, poor hiring practices can be costly. Companies can reduce their exposure by adopting and implementing the right hiring policies and procedures.

Among the elements to consider are how to treat the résumé, what to ask in job interviews, what information to seek on the applications, and what to consider in the job-offer stage. Addressing each of these elements wisely and legally are the keys to avoiding lawsuits.

KEY CONTROL PROGRAM

Previous issues of the Overland Security Briefing included an article on key control programs. This article has been rewritten and presented here. The second, and last, portion of the article will be included in the next quarterly issue of the OSB. Those requesting the complete article may do so by contacting Overland Security Services. This article will deal with the conventional metal cut keys used in 99% of businesses and applications we encounter.

The ring of keys each of us carries with us daily are truly "the Keys to the Kingdom." Each key is designed to open a device or lock specifically designed to prevent unauthorized access to an area, a door or gate, start a motor vehicle or other piece of equipment. By having access to that key, we are granted access to that area, room, asset or operation of critical equipment.

Often, we at Overland have asked for a key from a new client to permit us to enter a property or building. All too often, the client opens a desk drawer or file cabinet, pulls out a key and hands it to us. There is no record kept of the transfer of the key, who it was issued to, or what access was granted to the person receiving the key.

When we at Overland receive such a key, it is identified, tagged, then secured under additional lock and key and issued to only those with a need-to-possess that particular key. A written record of the chain of custody is kept, with everyone handling that key having to sign when receiving it. In this manner, we can identify the location of each and every key in our possession at all times. This is the standard of care we must exercise as stewards of these keys, and the access they grant, which have been entrusted to us.

Every key control program has the following main points:

- Identification of every individual key in the system.
- A record of every key issued in that system.
- A method of identifying what each key operates.
- Security measures to insure keys are not reproduced without proper authorization.

- Measures to insure that those individuals receiving keys understand the duty and responsibility that accompanies each key.
- A method of securing un-issued keys

Identification

When we are issued an individual key, we soon learn what it operates/opens without much thought. However, if we handle scores of keys for numerous locks installed in many buildings, we need a system of identifying individual keys and the locks they operate.

One system is to identify a building, or area, by the use of a unique identifier, such as a letter. The office could be "A", the shop identified by the letter "B" and the warehouse by the letter "C". In this manner, we can identify any key with the building it is associated with.

Therefore each key associated with a building will have that letter stamped on one side. Letter/number stamps are available from most tool vendors at a nominal cost. They are durable and will last a lifetime.

Within each building, each door can be identified by a number. An example would be that the main office door would be identified by the number "1." Using this system, the main access door for the office would be key A1. Therefore every key that opened the main door to the office would have A1 stamped on it. Other office doors would continue this sequence, with A2, A3, A4, etc.

If needed, a unique identifier for that individual key would be included. This might be as follows: A2A or A2-1 would be the first key issued, with A2B or A2-2 being the second, etc.

This system of identification is a suggestion. The system must make sense to the user. Any combination of letters, numbers or other symbols can be used, but they must be easily recognized by the users.

Issued Key Records

A record of keys issued must be kept and maintained at all times. Key control means knowing where keys are and to whom they were issued.

There are computer based key control systems, but we will touch on a simple paper based system. The basics are that every key issued must be signed for when issued.

The most basic record is a form stating that a key, identified by its unique identifier code, was issued and the form signed by the person accepting the key.

What does this key open/operate?

Often, and over time, there is no system of keying or record of locks installed, removed or changed over time. We simply end up with a ring of keys, opening a number of locks, some of which may have been changed out years ago.

For this reason, it is a good idea that once a key control system is considered, a general overhaul of all locks and keys issued be performed. When a system is instituted, former employees may have retained keys and current employees have keys to areas where they are not authorized access. This is a good time to survey the entire system of locks and keys; change or rekey existing locks and review who in the organization needs access to what areas. *To be continued*

The second and last installment of the article " Key Control Programs" will be included in the next issue of the *Overland Security Briefing*. A complete copy of this article will be mailed to any reader who send a SASE (#10) to the Overland offices at this address:

Overland Security Services
Key Control Program
PO Box 145
Santa Maria, CA 93456

OVERLAND 2, BAD GUYS 0

It seems crime never takes a holiday. A local vegetable grower had experienced several pallet thefts the first week in June. Over two nights, three days apart, thieves had made off with 150 new, unmarked pallets from the pallet yard.

On Friday, the 3rd, the grower contacted Overland to arrange for a surveillance to be placed on his yard. Overland placed a security officer in a hidden location that Saturday, and waited

At 12:58 AM, our officer observed a flatbed truck enter the property from the south and park next to the fence at the pallet yard. He waited and confirmed that they were, indeed, passing pallets from the stacks and loading them on the truck. He then called the Santa Barbara Sheriff's Department, who dispatched two units.

The suspects had apparently thought something was up and had driven off the ranch. Deputies caught up with them several miles west at Black Road and W. Main St. They were stopped, then handcuffed at gunpoint. The Deputies brought both suspects and their truck back to the scene of the crime to confirm their identity. Both then were taken to the County Jail.

Sheriff's Deputies reported that Darin Banks, 40, and John Hall, 53, were jailed on \$20,000 bail for the theft of 60 pallets. The case has been forwarded to the District Attorney's' office for prosecution.

The duty of security officers is generally to Observe and Report. In this case, their duties included identifying the vehicle and culprits.

Overland offers a variety of security related services to the Ag community. Mobile patrol service, stationary guards to

provide a visible deterrent to crime and sub rosa surveillance for specific applications.

Disposing of Employment Documents

Identity theft has been in the nation's headlines for some time. Reports of massive thefts of personal information from information vendors and credit firms have occurred as well as an increasing number of individual reports of identity theft.

Banks were among the first to realize that they possessed and handled vast amounts of information that could be misused, if measures were not taken to insure the security and safety of customer data. Since that time, most businesses have enacted policies limiting access to data and developing a formal policy for disposal of unneeded files, computer data and paper records. Simply discarding them away is not an option in today's world.

It is not sufficient to simply have a policy, it must be enforced. The employer/business must show that they have observed due diligence in insuring that records containing personal data be rendered completely unreadable or unusable.

In addition, confidential sections of employee files must be segregated from general employment information and access to that information restricted to personnel with a legitimate need for access

In today's litigious society, business owners and managers must take a proactive posture in insuring the confidentiality of client and employee records. To do otherwise is to invite disaster.

The following announcement outlines legislative guidelines for limiting access to confidential employee information and the destruction of data prior to disposal.

Starting June 1, 2005, employers wishing to dispose of employment documents that contain personal information must do so by shredding or burning them. A law passed in 2003, the Fair and Accurate Credit Transactions (FACT) Act, imposes the new requirement of all employers, regardless of size. The purpose is to protect current, past and prospective employees' personal information such as social security numbers, addresses, telephone numbers and any other information that is reported to an employer by a consumer reporting agency.

If such information is stored on computer disks or other recordable media, it must be destroyed before being discarded. If the data is stored on the hard drive of a computer that is being sold or donated to another party, the data must be removed in a way that makes it unrecoverable.

Employers also must restrict access to this information while being stored. Failure to comply with the new regulations could result in federal or state fines or civil liability in individual or class action lawsuits.

What Should You Do?

- Keep employee's confidential information (such as health data, background check results and credit information) separate from general human resources files.
- Establish policies limiting access to employee files containing confidential information and monitor compliance.
- Establish practices for the proper destruction of employment documents and electronic data and monitor compliance.
- If you contract with an outside provider for the storage and/or destruction of records, confirm that it complies with these requirements.

Armstrong's Lock & Key

In Santa Maria Since 1934
Sales-Service-Repairs
Commercial Residential Automotive
24 Hour Service
Locally owned and operated
Safes and Vaults • V.A.T.S & P.A.T.S

322 No. Russell Ave., Santa Maria, CA

Emergency/After hours Call 925-1050 or 922-3055
State Contractors License 548303
CLO # 623
(advertisement)

Overland Security Services, LLC 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. Edward J. Zemaits, manager, 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.

