INTELLENET NEWS

December 2006

Table of Contents

Carino's Corner

As I reflect back on this year, it was a great one for Intellenet. We had a most successful seminar in Calgary, we added quite a number of quality members and feedback received indicated that the Intellenet name assisted many in new business opportunities. Further, as this goes to press there are three international projects in varying stages of development that are fully expected to materialize.

Intellenet also continued to maintain its support with regard to other Associations. Many of our members are Presidents or immediate Past President of their State Associations while others are in key leadership positions in other international associations. In my judgment, these factors all contribute to the professionalism and growth within the PI field.
The year did have some downside, however. We lost two Board members with the passing of Gerd Hoffman in February and John Belrose in June. Additionally, two other long time members – Phil Guillen and Art Tredinnick also left us – in all cases prematurely. Each will be long remembered for their contributions to Intellenet and each will be missed in the days and years to come.

The year 2007 will bring new challenges and I am confident that Intellenet will meet them head-on. Expect to see a major push by NCISS for new members. Intellenet and its members are already large supporters – both membership and financial support wise but greater efforts will be needed if NCISS is to meet its objectives in achieving fair and reasonable legislation. As leaders in this vast field of nationwide/worldwide PIs, Intellenet members will need to intensify membership efforts and in ensuring that our profession's high ethical standards are met.

My best for a happy and joyous holiday season!!

Know Your Fellow Members

Geoffrey Hughes, PCI
Jell Group
Tunbridge Wells, N3 9ZH
England

Geoff Hughes is a native 'Brit' who conducts & manages international investigations and risk management projects around the world from his base near London. After a spell in marine insurance claims, in Vancouver BC, and 20 years in a secretive UK Government department, he became Operations Director for a well-established investigation agency before forming his own company in 1993, specializing in discreet, complex and geographically widespread fraud investigations. That company evolved into the Jell group, which now provides investigative services on both sides of the Atlantic Ocean, including Europe, the Former Soviet Union and Africa.

A longtime member of the British 'Institute of Professional Investigators' (IPI) and 'Institute of Directors' (IoD), Geoff is also the first European to obtain the US 'Professional Certified Investigator' (PCI) designation. He thus joined the small band of non-US investigators qualified to US standards.

While the business provides a full range of background checks and related services, his personal specialty is discreet in-depth overseas fraud investigations or troubleshooting missions for conglomerates, legal advisers and large companies based in the UK or USA; only a small proportion of his work is actually performed in the UK. Because most overseas projects are carried out in hostile conditions in 'third' countries, usually under cover of an unrelated business assignment, he has become adept at risk-evaluation and an expert on numerous foreign cultures, legal systems and commercial practices. This in turn has led to some interesting longer-term risk assessment assignments in African and former Soviet Union countries.

As if this lifestyle didn't provide enough foreign travel, including dozens of visits to the USA, Geoff is also a professional sailboat captain, taking small groups of adventurous travelers on custom tours of the Greek Islands, when other commitments allow during the summer months.

A proud member of Intellenet for many years, he bases his continuing personal development program on the outstanding education and networking opportunities provided by Intellenet, particularly through its annual seminars.

Police in Oakland, California spent two hours attempting to subdue a gunman who had barricaded himself inside his home. After firing ten tear gas canisters, officers discovered that the man was standing beside them, shouting out to give himself up.

Executive Protection in the New Century—A Brave New World

Ridge Marriott
Marriott and Associates, LLC
Northport, Alabama

LTC, USAR (Retired), Former US State Department (Inspector) and US Immigration & Naturalization Service (Special Agent)

My background both as a former Federal agent and "unconventional warrior “with US Special Forces; (MACV-SOG) and the Army's Terrorism Counteraction Task Force-as a green-suiter in the mid-80's-allows me to bring some effective focus on today's corporate worldwide challenge.

But a lot has changed in twenty years.

The protection goals of principal or targeted executives have remained relatively the same: How to economically protect an executive whether in the US or abroad, when a threat scenario or hostile environment occurs.

An additional requirement is effectively briefing and educating today's corporate clients. This could also be termed “follow-through".

It is the unlevel world-wide playing field that has undergone radical change. For the first time since the years of the Red Brigades and the Baader-Meinhof Gang of Europe-corporate interests overseas, particularly the Middle East and Latin America-must seriously factor in realistic protection of its executive management.

The wisdom of at least two of three Federal agencies may be drawn upon and utilized by both clients and the executive protection professional. As many are aware, the United States Secret Service is the hallmark agency charged with the protection of the Chief Executive and his family-in addition to visiting foreign dignitaries.

The US Department of State and the Office of Homeland Security both have a responsibility to provide current threat assessments for its citizens in certain cities locally or traveling management staff within regions of the world or individual countries. State Department advisories are general guidelines. With some diligent research-more specific intelligence or pertinent information may be obtained on a specific city within a country. For example: Tel Aviv, Israel; Bogotá, Colombia or Damascus, Syria.

In many cases, executive protection specialists work with host government agencies or local professionals who serve as both intelligence sources and executive protection assets. It is these assets that will sometimes make or break effective threat analysis and protection teams.

One of the interesting maxims that come out of executive protection work, especially among corporate clients in the United States is "they love to see you arrive and then they love to see you go". This is directly related to the "success" ratio of your service to the client; it also is a left-handed compliment. Professionals get their own reward. It was years in law enforcement before I REALLY understood what that meant.

The length of the "protective detail" ideally should split the difference between what the client wants and what the professional convinces the client he really needs for his specific protection requirement. "The customer is always right"; well, maybe at Lowes or Nieman-Marcus. Educating the client is part of the implied contract. In a well-run executive protection detail, the client or protected principal will come away from his or her experience with a new-found appreciation of both how vulnerable they may be in today's society and how valuable your services are to their well-being.

In the 1980's, Princess Diana and Prince Charles went through an extended training period with the SAS (Special Air Service) at their Headquarters in Hereford, England. Both were intensely impressed with both the quality and detail of the protective service provided by the SAS to the "Royals". The SAS continues to enjoy an enviable reputation worldwide for their protection efforts.

Our own Special Forces Operational Detachment-Delta trains and organizes its efforts along SAS Squadron guidelines. Like the SAS-The Israeli Secret Services including the Mossad place a great deal of influence on realism and very current-reliable intelligence information. Of all the important factors in executive protection, reliable and timely information and intelligence is chief among "sine qua non" requirements. Absolutely trustworthy staff, technological and language capabilities rate highest.

Executive protection is ideally a great deal more than warm bodies placed at likely avenues of approach or threat. It is infinitely more than "bodyguard" assignments as visualized by a growing less-than-intelligent general public.

As world trans-national terrorism continues to mount, corporations will continue to need our services for their key employees. Observing the security measures change in U.S. airports following the 9/11 aircraft hijacking are indications of complications that must be currently dealt with by professionals. In many cases, these types of security measures are marginally effective against a threat-but they may cause more problems for the clients and protective staffs. Specifically, these same measures may obviate the use of imported technology or any use of firearms, even when provided by the host nation or clients-without permits or special licensing.

A well-known and respected investment firm began to have interesting reactions among its clients to the down turn in the stock market from the .com bubble and other market factors. Threatening behavior was one reaction, complete with very real unpleasant confrontations.

As in this case, large corporations with certain customer difficulties cannot afford the negative publicity of unwise contact with local law enforcement. As many of our members are aware, law enforcement agencies can be helpful and supportive or they can be a decided hindrance and part of the problem.

It is always wiser to keep liaison active and cooperation keen in advance of an anticipated need of law enforcement interaction. Unfortunately, this can be difficult with larger departments or conflicts in scheduling. Back to Rule 1-Maintain friends of influence within law enforcement circles and keep them.

CASE HISTORY: At a large corporation a certain supervisor developed a relationship with a female coworker. The woman decided to end the relationship. Complications arose when the male supervisor did not wish to end the relationship-complete with paranoia. As a 15-year career-track employee, he was first counseled by management and then given a 30-day suspension. Failing to learn from these experiences, he was finally given notice and terminated for on-the-job harassment of the female employee. After termination, he threatened the female employee. More specifically, he threatened the Assistant Plant Manager and his family with death threats. He also made the same threats to the plant union president and his family. For two weeks, assisted by a retired FBI agent, my firm provided executive protection for these employees in rural Alabama. Finally rumors reached the terminated employee that Sheriff's deputies were watching him and the plant employees during working hours; while former Federal agents were protecting the families and employees at their homes at night. (Note: Since this was December, hunting season was in full swing, with camouflaged deer hunters within 200 yards, were walking in the vicinity of the concerned employee's house. One residence was in the "outback".)

Around-the-clock protection was provided, the situation resolved itself and for once the local plant employees really wanted us to stay, regardless of the cost to the company. A happy ending resulted and good will affirmed within the community. It was very rewarding with a sense of real achievement. Another added benefit is that the successful resolution of a difficult case/detail in executive protection gets around in corporate circles as well as among our own professional organization.

Liability Insurance

Bob Yergey
Yergey Insurance Company
Manassas, Virginia

This article will be more focused on some parts of a basic general liability and errors and omissions policy. Below you will find some information to use when searching for a policy that will fit your needs.

Not all policies are alike. The fact is most policies are based on relatively similar basic forms of coverage. However: endorsements, exclusions, and conditions can make these similar forms move worlds apart. Be sure to review your policy for how the exclusions section changes the coverage under the other sections of the contract.

Under general liability, security and private investigative industry products provide coverage for unintentional acts of bodily injury, property damage and personal injury. Bodily injury can come in the frame of an accidental injury to a client or subject caused by the negligence or non-negligence of one of your employees. While intentional acts are excluded, most security contracts contain provisions for assault and battery to be included in the policy coverages. Private investigator specific contracts might not have the assault and battery coverage since this is not as applicable as in the security industry.

Property damage will result from the accidental damage to a third party's property while in the course of work. Be advised that this coverage and all coverages that we will discuss exclude any damage or injury due to automobile causes. We will discuss auto liability in a future article.

Personal injury coverage is afforded under most general liability contracts. This can vary by industry but is an important coverage when you are working with the general public each day. This coverage affords libel, slander and defamation of character coverages and has been a popular target for plaintiff attorneys in recent years. The coverage should be included and should not have any form of its protection diminished by endorsement. In some cases, personal injury is excluded. Certain high-risk industries and companies using the Internet for their services can have trouble obtaining this coverage.

Most policies contain medical payments coverage, which can be used to appease an injured subject to avoid a liability claim. This coverage is used to pay small medical bills and costs associated with injuries for third parties. It can be an effective deterrent to utilize this coverage to convince a claimant not to file a lawsuit. Use of this coverage does not preclude a person from filing a liability claim but can sometimes prevent this from happening.

Fire Legal Liability is an often-misunderstood coverage. This coverage is also on most general liability policies and is designed to protect the insured from damage to a rented premises through events caused by an insured. The coverage will pay for damages to a structure that you rent but do not own. For this coverage to apply, gross negligence would have to be proven. The best example is the coffee pot left on overnight. Should this occurrence cause damage to property not owned by you, coverage could apply.

General liability policies will in most cases carry a deductible. The level of this deductible can vary and is usually negotiable. Raising the deductible in some cases can reduce premium levels. Be sure that you are aware as to whether the deductible applies to defense costs or just indemnification.

Lastly, these policies can come in two formats for claims reporting. First, an occurrence policy allows for an unlimited period after the policy is no longer in force for a claim to be reported. The cost for this type of policy can be more expensive at times to make up for the future reporting of claims.
A claims-made policy has a limit as to how long after the policy a claim can be reported and covered. In both cases, occurrence and claims-made, the coverage aspects are similar and the claim must occur during the time the policy was active. However, after the end of a claims-made policy the insured must arrange for the extension of the time a claim can be reported. This can cost additional premium and must be purchased shortly after the end of the policy expiration.

Future articles will include auto insurance, workers' compensation, property, business income and many other aspects of insurance that firms of all sizes should consider.

A Cop Party--Surprise! Surprise!

off the mark
by Mark Parisi
www.offthemark.com
BEST COSTUME, HERE I COME!
POLICE DEPT. HALLOWEEN PARTY
MARK PARISI
ATLANTIC FEATURE © 1996 MARK PARISI
www.offthemark.com

ARF, ARF…GOT YOU

Sgt. Silicone
Reprinted by Request from Previous Intellenet Newsletter

Editor's Note: Obviously, Sgt. Silicone is a pseudonym of a computer expert. He/she may be contacted through the Editor if anyone has any questions concerning this article.

If you have obtained software for your computer and in running that software had the message

"ARF, ARF"...GOT YOU" appears on your screen, you have a real problem. You've just been hacked. A hacked computer program is one that is unlawfully modified or designed to purposely mislead the user into operating that program with results that are other than expected by the user. Hacked programs can be as benign as putting in a message in the middle of the program such as the hacker's every popular "ARF, ARF" (not overtly destructive, more of a means for "counting coupe") to erasing vital information necessary to the functioning of the computer, or, in some instances, actually causing physical damage to the computer. Hardware sabotage via booby trapped software can take several shapes. IBM-PCs are susceptible to having their read/write head repetitively banged into the media and end stops. This results in the computer's drive being as useful as a pencil with no lead. Another form of destructive software can overload the active control bus (this is the system that sends the commands in the compute to make it do all of its tricks) by turning on and off all the circuits in a rapid succession, causing burnout (somewhat similar to a lobotomy, but more permanent.)

But hacked programs don't stop at just destroying equipment and hours of work. More insidious is the use of hacked programs to "acquire" the data kept in someone else's files. This is easier to do than most people think.

If the computer being attacked has an accessible termination to the attacker (i.e., in the same building or office, or a remote terminal in another more accessible office), the job is made very easy. If a password is used to access the levels of the system desired, that is the first thing that must be obtained. Most people write their password on something and keep it near their terminal. Passwords can almost always be found in trash bins outside of offices. Social security numbers are the most frequently used passwords, followed by family names, phone numbers, sequential alpha/numeric combinations (123456789, ABCDEFGH, 1111111, etc.) But why bother with all of that work when you can get the system operator to give you the password. One method used is to write a Trojan horse program and enter it into the system using a known lower level password. A Trojan horse program is, as the name implies, not what it appears to be. In this case, this program will appear on the VDT (video display tube) when your target goes to use it. It will resemble the usual sign-on sequence the user is familiar with and will ask them for their password to give them access. But, the Trojan horse program will take that input, the user's password, and store it for the hacker's late retrieval. The user will receive a message from the computer asking him to try his password again due to "error" in input, and this time, the program will have defaulted to the original correct program asking for the password and the user will go on his merry way, little realizing that he has just given his password to someone who will be able to successfully impersonate the legal user of that password (and access data, transfer funds, destroy data, etc., all under the legitimate person's password). Passwords are also obtained by hiding Trojan horses inside of "attractive" public domain software (subtly altered to contain the Trojan Horse program that either instructs the system that downloaded the program to accept another password—the hacker's). This is particularly effective in "unlocking" someone's "mailbox" so that you can read their electronic mail, or delete all of their files, or even put a bomb in their system.

A logic bomb is a modification to a program that already exists in the target's system. It just sits there until a specific set of circumstances activates it (a passage of a specific amount of time, even years, the running of a particular program, etc.) Upon being activated, the logic bomb can order the computer to alter files, destroy data, lock out specific users (somebody the hacker is "unhappy" with) or any variety of commands that come to mind. The logic bomb is particularly difficult to find, in as it can be planted just about anywhere in a computer's software and can even be programmed to move itself to different locations in a system in a predetermined manner to further avoid its being found. Logic bombs are particularly effective for providing insurance to employees. They can be set, so that if they are not "treated" by the person who planted them on a regular basis (for example if the employee gets fire" they go off. Not only can heinous damage be cause to a company's records, but the employee's personal files can be deleted in one fell swoop. Finding the provocateur is almost impossible. One instance occurred where the planter of the logic bomb turned himself in to his employer after setting up logic bombs throughout his employer's system (in the operating system, utilities, data files, etc.) He

called the top management together and explained to them that unless he personally defused his logic bombs in a manner and schedule known only to him, he could and would shut down the company. It took only one demonstration to convince. His salary was doubled, a large “bonus” was provided and he received a lifetime guarantee (in writing!) of his employment. Every now and then, he even comes to work to defuse one of his logic bombs.
Access to the knowledge necessary to make Trojan horses, logic bombs, etc. is easily obtainable. Large quantities exist in the public domain, I PC magazines and on hundred of electronic bulleting boards across the country.

One extremely well organizes BBS is 2600, a compilation of five BBS systems with a parent, quarterly Magazine. They can be reached at (516) 751-2600 (not in service on 10/01/2006). They are located in Middle Island, New York. It costs $15.00/year to subscribe. Caveat emptor, however. While numerous quality computer people are members of 2600, there are some pranksters as well as several law enforcement organizations that routinely monitor these bulletin boards.

Hacking, particularly with the advent of new Federal and state legislation has in many instance come under the umbrella of the criminal code. Unfortunately, because of the very nature of the activity, 99% of computer crime is never discovered to be criminal in nature or even found out. What usually happens is non sabotage oriented computer crime is that money just disappears. No trail to follow, no evidence, not even a crime scene. Those who do get caught usually fall into one of several categories:

(1) A small time employee who happens to have access to a terminal with a minimum of safeguards. This person, while possessing enough knowledge to do his/her job on a terminal, usually lacks any computer of programming expertise. Usually, the crimes involving these people are of relatively low monetary value and involve increasing or decreasing dollar transactions and deleting transactions altogether. Additionally, this person may play with product or consumer orders sending material under fictitious identities to confederates or themselves. Jerry Sneider is an example of this category. By going through Western Electric and Pacific Telephone and Telegraph trash bins, he obtained passwords and purchasing procedure document. He then set up a company ordering large quantities of parts and equipment from Western Electric and Pacific Telephone and Telegraph and had them sent to himself. He then sold the equipment to various companies. Had he not infuriated one of his employees who was aware of the scam, he might still be in business (or retired comfortably). It’s he stole over a million dollars. His biggest customer was Pacific Telephone and Telegraph. They never knew they were buying their own equipment back. When caught, Jerry confessed and was convicted. He served 40 days in jail at a minimum security facility in Malibu, California and was fined $500.00. He now has a five figure income as a security analyst. That will teach him!

(2) Bright kid (gone bad?) make up the second category. There are lots of examples of these. Other than using their talents to steal free phone time and occasionally getting some “acquired” computer equipment, they are more scary than larcenous. They like to access systems they aren’t supposed to, sometimes leaving little messages telling their target they got in their system (“ARF, ARF” or the ever popular “Gotcha”). Occasionally, they will vandalize their target’s files and programs. Recently, a well publicized hack involved a graduate student planting a virus that eventually entered hundred of systems around the country.

One of the most interesting examples of this category was the 414 gag. A bunch of bright kids led by two 14 year olds, Gerald Wondra and Neal Patrick, entered the Security National Bank and several others. They were eventually caught because a particular savvy computer security person recognized the access attempts as being the type performed by kids (he noticed that they weren’t actually trying to steal anything or destroy data). Attempts to trace phone calls used to access the systems were ineffective because the “kids” worked through other unsuspecting computers to gate (or reroute) their calls. They were finally caught when a Star Trek type game was put in one of the target computer’s menu. This game was so intricate and involving that the kids stayed in the system for almost two hours playing the game, giving the authorities time to trace phone calls from computer to computer until it came back to the hackers. They were all given two years probation and told not to do it again.

In 1982, two teenagers, Ron Austin and Kevin Poulsen, penetrated Arapnet, NASA a Pentagon computer systems with a used TRS-80 computer. Arapnet links together the US Government's scientific and military computers (in excess of 5,000 entities) across the country. They used a simple Trojan horse on a computer system at US Berkeley (first finding the password, UCB). It took them four tries to figure that one out.) Then by using a Trojan horse to capture log-on names and passwords, they eventually captured the I.D. and password of someone who had access to all levels of the entire Arapnet system nationwide. The only reason they were caught is when one of the teenagers put in his own real address when he was ordering something from one of the entities he accessed. Hopefully, he wasn't ordering plutonium or anything like that.

(3) The most successful category of hacker is the most dangerous. They are rarely caught and few of their crimes are unearthed. They steal the most money and usually suffer the least consequences in the rare instances where they are found out. They are usually a professional person and/or a member of upper management. They are well educated and have a good income. They are usually caught because they made a simple error they overlooked or are turned in by a wife, confederate or fellow employee or they got drunk and bragged about it to somebody.

Probably the largest instance of this type computer hacking/fraud occurred when officers of Equity Funding Life Insurance used a computer to fabricate two billion dollars worth of phony accounts. They programmed their computers to invent 64,000 fictitious customers. They made their money on the scam by selling shares in the company to unsuspecting investors who were given this portfolio outlining their "large" client base.

In 1988, the FBI, Bell Security and state and local law enforcement raided a popular bulletin board group called SBBS in Santa Clara, California. This group terrorists managed to accomplish the following in a short period of time: shut down the Pacific Telephone traffic position office, totally access the California Department of Motor Vehicle Records, penetrated several computer companies' records, (including DEC), penetrated Arpanet (the computer network referred to earlier that is run by the Department of Defense), accessed NCIC, accessed a variety of airline reservation computers (they took to heart the motto "leave the flying to us" and acquired unlimited free airline tickets) and generally played havoc with systems across the country.

The list of abuse is lengthy. The list of unfound abuses is much, much longer. Means to counter illegal and improper access to computer systems are constantly changing. The Tempest Program provided by the US Government to harden their systems is effective in a limited sense. But, as of 1986, in the government sector alone, 25% of surveyed government agencies did not screen employees who access computers. About 40% of the government agencies survey (cabinet level departments, and 20 independent agencies) had not conducted risk analysis studies of their computer systems in the prior 5 years, 75% did not have explicit microcomputer security policies and 60% did not have plans to protect data if their computer systems were disrupted. The private sector is even more dismal in their approach to security.

A new generation of software has been developed by a variety of sources to counter the threat posed by the hacker worms, viruses and time bombs. They include: Bomb Squad, Flushout+, Cylene-4, Check for Bombs and Mace Vaccine. Cylene-4 is particularly effective and is available from Interpath at 4423 Cheeney Street, Santa Clara, California 95054. They are all reasonably priced (less than $40.00 and, by and large, are quite effective). However, the insidious hackers have taken some of these vaccine products and changed them with Trojan horses, then made them available for free on various bulletin board systems. One example of this is Flushout 4.ARC. Run this little baby to check for problems in your software and you will end up with a trashed disc. A host of data encryption programs are now available limiting the use and value of data purloined by the silicon thief, and, in some ways, further limiting access to systems. Various hardware add-ons are available making access to systems more difficult.

Computer are fantastic extension of the human mind, allowing tremendous amounts of work to be done quicker and better than ever before. They are here to stay. So are the hackers. Protect yourself.

Designing a Comprehensive Security Program

Carl G. Hatton
Hatton Industries Security
Greeley, Colorado

The business owner or senior executive normally does not have a security background and must rely on others for professional advice, program implementation and management. A basic understanding of how to design, implement and manage a comprehensive and viable security program within the financial constraints of business will ensure an appropriate response to your needs without fear of manipulation of security costs, and environment for unwarranted security vendor advantage. It is best to remember the old adage—"you get what you pay for!" Carelessness and incompetence equals financial loss and increased legal liability.

What should be protected?

Many times, the only security implemented is the installation of security cameras and access control devices. These devices can assist in protecting the physical property but this is not your most valuable asset. Your MOST valuable asset is the reputation of your company: on the outside from the general public and from your employees on the inside. Essential to your reputation is how satisfied your business customers and employees feel when they are on your property. The mere appearance of security officers and devices may give a false impression of the safety and security situation on your property. It is the quality of performance of these devices and individuals that is the true test of your security precautions. As a business person, nothing less that professional performance should be an acceptable standard. The key to protecting and promoting your company's reputation is not your name, the type of business or the appearance of cosmetic solutions to perceived problems—it is the people who are your customers and employees who shape your reputation.

What are the components of a comprehensive security program? The comprehensive program consists of interacting, interlocking and overlapping features that provide mutual support and direction of the program: devices, personnel, policies and procedures, education, inspection and management.

How do I know what I should have within my security program?

Before starting to identify what you need for a viable program is determining what are the threats to be faced and neutralized. This is accomplished through a comprehensive risk assessment. Not only the internal risks facing your business but the external threats affecting how you safely do business.

The internal threats can range from the manufacture or use of hazardous materials, the presence of pharmaceuticals, and availability of pilferage of high value products and supplies and similar items. The external threats encompasses criminal activity adjacent to your facility, the demographics of the neighborhood, ease of public pedestrian and vehicular access to the facility and neighborhood, and the service quality of area public safety agencies.

A big mistake to make during your risk assessment is depending on supervisors and manager to be the sole input source of internal information. Frequently these people only know what they are told by their subordinates—therefore directly to the source of the information. Some managers will manipulate the information for their personal benefit.

Direct contact with your employees provides you with first hand information from their perspective and gives them a feeling that you are concerned for their safety and security as well as providing employee "buy-in" for your solutions. The use of a confidential employee questionnaire gives the best results. Much valuable information will be lost if the employee feels he/she can be identified as the information source. The information provided may not be the most valuable input you will receive but it gives the employee an opportunity to vent as well as feeling that their comments are important. The providing of the information has more value sometimes than the actual value of the information.

Information of external threats can be obtained from public sources and personal observations. The quality of public information cannot be guaranteed to be 100 percent accurate because of possible political manipulation, agency competency, and manpower considerations. Observations of a trained security person may have more value.

How do I ensure our program is adequately comprehensive?

To be comprehensive, your security program must consist of interdependent parts with the ultimate goal of supporting the overall program objectives. Inanimate objects such as security cameras, fences and gates, and access devices cannot be effective without human intervention to guide expectations. Therefore written policies and procedures are a vital element in the equation. Policies express corporate expectations while procedures provide the conduit for policy implementation. In the unfortunate event of civil litigation of loss for injury on the property, the policies and procedures are critical to successful defense strategies.

Successful policies and procedures require that they are capable of being implemented. The policies cannot prescribe utopian requirements that cannot be implemented due to lack of necessary equipment, training and personnel. Policies and procedures that can be easily implemented when the majority of working staff is present may not be capable of implementation at night with drastically reduced staffing levels. Therefore, alternate strategies may be necessary during different portions of the workday and workweek.

They only way the viability of your directives can be measured is through continuing and comprehensive testing. For example: testing of the fire evacuation plan after significant notice to staff members does not provide a true picture of the plan's viability. Employees, knowing that the plan is to be tested, will review the plan ahead of time, plan their work and smoke breaks to coincide with the execution time and in many cases will have evacuated the facility before the actual beginning of the test. Unannounced tests provide much more valid information.

All policies and procedures should provide the following answers: who, why, what, when, where and how. The procedures should also identify the location of all equipment necessary to successfully complete the plan expectations. Identification of assembly areas and personnel accounting, both employee and visitor, must be part of the evacuation plan.

How do I identify and evaluate security devices?

Once expectations and goals have been identified, it is time to identify your physical equipment needs. It is advisable to utilize the services of a qualified security consultant to identify your general requirements. Brand name products should not be identified as a requirement of your specifications. Identified vendors should be allowed to use any product that meets your needs. The brand name does not guarantee that it is a wise cost-effective choice for your business. Service vendors and suppliers have different purchasing agreements affecting cost and the same brand name product may be more costly to different vendors. Direct from the manufacturer purchases will be less expensive than having the additional costs of various layers of middlemen. It's also wise to have agreements with vendors on the expectation and warranty of the equipment provided and installed.

It is important to have all potential service providers be present for a bidder's conference where areas of protection interest are explained to all providers at the same time. The potential vendors should be shown were and what type of protection is desired without being told the specific devices to be used. For example: they should be told that visual protection is desired in a particular and specific area but not what type of device should be installed. Identifying the proper equipment to meet your needs is part of the vendor bid process. There are instances where they may provide input that complements supplements or exceeds your initial expectations.

As part of the bid package, the vendor should be required to provide a list of previous installations with contact names of the responsible parties. This allows the purchaser to contact these individuals and determine their satisfaction with the products and installation. Upon receipt of bids, the proposed devices should be rigidly checked to ensure that they are capable of meeting their expressed capabilities. The successful bidder should be required to outline in detail all warranties as to the product and his installation.

Device installation must be in accordance with applicable law, regulations and ordinances by certified and technically qualified individuals. Some jurisdictions require permits and licensing. Further, you should receive copies of all insurances and bonds before any work is started. The use of day laborers and non-qualified technicians should be expressly prohibited due to the potential for liability for faulty installation and devices.

How can I control the cost of security equipment?

Cost containment may be achieved through integration of security system input with some non-security systems. For example: time and attendance information can be obtained through integration with access devices on exterior doors or dedicated terminals, negating the need for two separate systems. It can also be utilized to manage facility heating and air conditioning systems through common timing devices. Thinking of the future and ease of integration now can save thousands of dollars in the future. For example, it's best to have extra room for pulling wires in conduit than not enough.

Duplication of security coverage can be a problem. It is not necessary to have expensive locks and security devices on entrance under 24/7 surveillance of a security officer. The type of security control at a specific entrance or area may consist of several possibilities. For example: an entrance door can be controlled by a security officer, a restricted entry access card or key, photographic coverage with entry authorized from a remote location, among other methods. Costs and exposures will determine the most appropriate security measure.

Adequate warranties and service plans are an integral part of ensuring proper functioning of security devices. As a minimum, each device should be inspected for proper operability by a qualified technician at least semi-annually with a requirement that written documentation be provided certifying that all devices are functioning properly.

How do I identify a responsive and qualified products and services vendor?

Identifying responsive service vendors and quality products requires that the vendors' marketing material be questioned. The satisfaction index can be identified through contact with previous customers and technical research. It is best to remember that the name of the vendor company and product does not guarantee quality of product or service. The best product installed in a haphazard manner is worthless. Having equipment that does not function properly increases your liability potential many times.

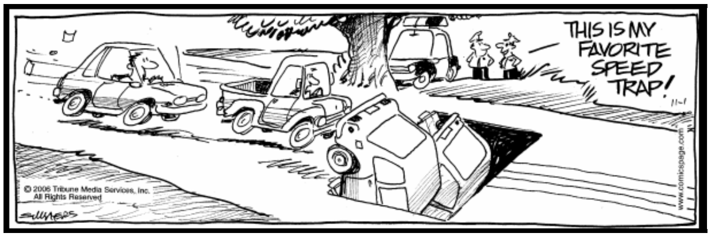
Whether you are in contact with a product or service vendor, it is essential that you identify their credentials. Some states do not have security licensing laws, allowing unqualified persons to enter the market, and with an impressive marketing scheme, become a profitable business. The question is whether or not they will be around when you are engaged in civil litigation because of a failure of their products or service. Again, you get what you pay for!

How do I insure the continuing proper operation?

All security devices should be tested on a periodic basis depending on their frequency of use. Operational characteristics can be checked by anyone, however, inspections of equipment such as alarm systems, fire pumps, etc. should be conducted by qualified technicians at least semi-annually, or at lesser interval as required by local laws. Every inspection, regardless of frequency and inspector, should be documented and retained for the period of time its production could be required in civil litigation.

The key to proper and successful utilization of a security program is management involvement. Subordinate managers can be tasked with the conduct of periodic inspections but senior executives should actively investigate to ensure compliance with corporate polices and procedures. Don't merely take the word of subordinate managers—be an executive **manager**! If you check on the checkers, the checkers will check on the equipment and people.

Innovative Traffic Enforcement--2006


THIS IS MY FAVORITE SPEED TRAP!
11-1
© 2006 Tribune Media Services, Inc. All Rights Reserved
SUMMERS
www.comicspage.com

"Field" Work

Geoff Hughes
Jell Group
Tunbridge Wells, UK

The brief was fairly standard, the kind of assignment many of us have had, many times. An international company, based in Europe, was suffering transit losses on a regular supply run between a central storage depot and consumer outlets. Suspecting an inside job, the company called me in to conduct a 'clean' investigation. I was given 10 days to complete the task, including reporting to Board level, based on nothing more than the internal auditors' assessment that a relatively small loss (about $200,000 annually) would take a relatively short time to solve. I had long since given up arguing against the 'one size fits all' approach to investigation budgets with this regular, if demanding, client.

The detailed brief: The problem was in the client's subsidiary company, in Gabon, West Africa, where fuel oil for the company's oilfield operations and production facilities was issued from central storage tanks in Port Gentil, the nearest international port. Quite simply, the quantities received at the various end-user outlets fell short of the amounts issued from Port Gentil (PG). Suspicion rested on the small general-cargo vessel which took supplies from PG to the main distribution tanks at a small port about 200 miles south; it operated to a regular weekly timetable, allowing three days for the voyage, which was perceived by management as being overly generous - and creating opportunities for illicit discharges *en route* without affecting the schedule.

Officially, my assignment was, acting as a Head Office auditor, to observe the distribution process, from PG to end-users, identify weaknesses, then make recommendations. The key objective, undisclosed to all but the local CEO and CFO, who had discreetly called for outside help, was to investigate losses so - as the culprits could include people at any level within the company - head office decreed that my exact itinerary would have to be secret. This meant I could not use the company's administrators for travel arrangements, support or research. The 10-day clock would start ticking with my departure from my UK office and end with delivery of the report. "Oh, by the way, you're needed on site on Monday morning." (Today being Tuesday).

So far, so good. A straightforward assignment in an interesting part of the world, in a warm climate and, although I hadn't been to Gabon before, I had sufficient experience of the region (Nigeria, Namibia, Zambia, Zimbabwe) to be aware of the likely hurdles.

Preparation:

Check travel requirements. A visa was needed so, as I was not officially 'invited' by the Gabon company, a suitable invitation letter was obtained from the parent company in UK and, using that, I obtained my own visa from the London embassy. The whole cocktail of jabs was required for entry to the country (Polio, Hepatitis, Yellow Fever, Typhoid, Rabies, *etc.* and prophylactics for malaria). It's not just for personal protection; the host country doesn't want diseases such as Yellow Fever imported, so it's mandatory.

Check local public holidays. I wouldn't be very popular with the client if local business closures gave me unscheduled time off at their expense.

Check local factors. French is the working language, with English also used *in some places.* Nevertheless, the client, being European and based in London and The Netherlands, used only English and all its subsidiary companies around the world were managed by English-speaking expatriates.

Make travel arrangements. I was required to meet the CEO, CFO and selected managers in Port Gentil at 10 am on the Monday, before observing the scheduled loading of the vessel at midday. Gabon being a former French colony, the only direct flights were from Paris, not London, so I booked to leave London at 8pm Sunday, change in Paris to the Libreville flight (Libreville is Gabon's capital city - and has the country's only international airport), then take an internal connector to Port Gentil, arriving at 9am Monday. This was communicated to the CEO, who arranged for his driver to collect me at the airport.

All this, and not a chargeable minute until Sunday evening!

The trip:

Armed only with the CFO's contact data, I made the overnight flight to Libreville, then on to PG, where I arrived on time, almost to the minute. At the exit, numerous local drivers with the usual name boards awaited the half-dozen or so expatriates from my flight; none of them were displaying my name. OK, perhaps the locals were playing it low-key; I couldn't complain about that. After about half an hour, I was the only foreigner in sight - and still no driver. I was repeatedly approached by helpful locals offering me lifts 'into town'. I politely declined, much to their amazement (apparently everyone knows each other, and they share transport; no-one waits around if their driver fails to appear). A call to the CFO's office informs me that my driver waited for 30 minutes, then returned to the office! A rather disbelieving administrator agrees to send him back for me. 'He'll be there in 10 minutes.' Twenty minutes later, I call again - and he has just returned to the office for the second time. A lengthy and ill-tempered conversation finally reveals that there are two 'terminals' (each the size of a large house); one for public flights and a private one for oil company charters. Having made my own arrangements, I arrived with the *hoi polloi* at the public terminal; my driver, having been told simply to meet me 'at the airport,' went where he always did - to the private terminal… If I hadn't had a '3G' cell phone with global roaming, I would probably still have been waiting there now!

We dropped my bag at the office and collected the CFO, *en route* to the oil terminal, to catch the vessel's loading operation at 11 o'clock. My briefing (short version) took place in the car - and I'd missed the CEO, who was flying out at 11:30. The most important news to emerge was that, with the country virtually covered in jungle, transport was in short supply so my itinerary would be dictated by transport timetables, not investigative needs. The whole trip had therefore been mapped out for me and I would have to do my best within the itinerary I'd been given. So much for the secrecy demanded by head office… After a quick introduction at the quayside to René, who was to be my guide and assistant for the whole assignment, we started work. *No time to wash, change clothes, get my bearings or refine my approach in the light of the 'briefing.'* Regardless of the supposed routine nature of this routine audit, I was clearly being treated as the bigwig from head office, with operatives almost clicking their heels as they came to attention when I approached. So much for low-key!

At about the same time as I was making my first significant discoveries I realized that, although this company was run by English-speakers, the working language was French. This little gem had been omitted from the brief! My working knowledge of French was to be put to the test, while I thanked my lucky stars the job hadn't been assigned to one of my German- or Portuguese- speaking colleagues. That would have been interesting…

Coffee was served in the captain's quarters around midday, when I finally had a chance to take stock, learn something about the company's fuel-oil distribution network and to evaluate the task ahead. Everyone assumed I'd been fully briefed in London (whereas those in London assumed I'd be briefed in Gabon…). I therefore did my impersonation of someone who knows what he's talking about, while taking every opportunity to invite the locals to give me detailed accounts of their roles and responsibilities. That's what I call a steep learning curve!

As he dropped me off at my hotel late that afternoon, René, who had obviously been comprehensively briefed on this 'auditor's' itinerary (I suppose it was a good job someone had!), announced that we were scheduled to visit at least five main distribution points during the next 10 days - and the flights had been booked!

He revealed that virtually the only commercial flights within Gabon are between Libreville and PG; everything else is private. Company auditors always travel on the client company's aircraft, which operated to a tight (and heavily booked) schedule between headquarters, oil terminals, refineries and remote jungle drilling/production sites. Our first journey was to be tomorrow morning; to operations HQ about 45 minutes flight away. Before that, we had to interview the head of oilfield support services in PG; René would collect me at 0800 (that's 0600 to my sleep-deprived body). By next morning, our interview had developed overnight into two meetings; one as described yesterday, the other with the Administration Manager in charge of accounting for GasOil (local name for diesel) - and we still had to catch the 11:30 flight.

I think by now you have the picture - there's no such thing as a fixed schedule or program; everything in Africa is subject to last-minute change and unpredictable influences.

The next week or so was a non-stop flurry of activity, working from dawn (6:15am) 'til dusk (6:45pm). The investigation itself would fill a book, so this is just a taste of the experiences.

The first precautionary measure comes at breakfast on day one. Avoid the dairy products: they may be well-presented in a bed of crushed ice, but they may also have been stored outside - at 90 degrees! Of course, 'dodgy' food is to be avoided at all times, but it's not always possible; after all, we have to eat something! Even when dining in company-provided facilities, you can't be certain that the local supplier of prepared chicken, for example, hasn't found the odd gopher, rat or other small jungle creature to boost his margins. Similarly, staff that live in mud huts (literally) can't be relied upon to stick to company hygiene rules all the time.

African aviation is legendary, and horror stories abound; most of them are true. En route to the airport we pass what at first sight looks like a tired Boeing 737 parked about 300 yards from the end of the main runway and about 100 feet from the road. Unfortunately, that location is a deep gulley full of tropical vegetation which, on closer inspection, can be seen growing vigorously through the broken windows and holes where the engines used to be. In reply to the obvious question, René advises that it's been there since last year, when it ran out of fuel a few seconds from home, landed in scrubland and slithered into the gulley!

We check in at the company terminal, to be told that our bags will have to follow on the next flight because this day's crop of returning expats has brought so many heavy bags that the plane can't carry them all. First come, first served. Or rather, he who bungs most travels with his luggage. From the departure room (seats for 10, standing room for 20), we see our empty aircraft slowly taxiing away across the airfield. Something wrong there, surely; we arrived the requisite 30 minutes before takeoff and were checked in within 10 minutes. After another 20 minutes or so, the plane returns and we board straight away, then receive an explanation from the captain - the refueller was a bit overenthusiastic and put too much fuel aboard - making the aircraft too heavy to take off, so they took the plane to a remote part of the field and burned the excess off by running the engines for a while!

Apparently no-one was fazed by this, as we all stayed in our seats and off we went. About 25 minutes into the flight, the noise level increases dramatically, followed by the captain's voice. "You know about the little fuel problem we had; well we still have a bit too much to make a safe landing, so we're increasing our consumption by lowering the undercarriage and extending flaps while we circle until we are light enough to land."

Outside Libreville and Port Gentil, the roads are mainly quiet and the biggest hazard (literally) is wandering elephants, which can often be seen ambling across the road or, worse still, dashing out of the jungle and charging across. All drivers of company vehicles must have defensive driving and survival training - and all vehicles are fitted with speed limiters, warning beepers and, of course, radios. This isn't just precautionary. On a three-hour journey, mainly on unmade trucking roads cut through virgin forest, to the terminal where the vessel inspected in PG discharged, we saw just 2 other cars. Serious accidents are all too frequent, with cars sliding off the dirt surface into the trees and not being found for days.

Expatriate oil workers are no layabouts. They are all under heavy pressure from budget-conscious head offices to produce more, in less time and with fewer resources - so the last thing they want is an auditor poking his nose into their domain. This works both ways for me; on one hand it can take for ever to locate necessary papers or information, on the other hand it's easier to follow an investigative trail without people asking awkward questions, because they have more than enough to keep them otherwise occupied.

Nevertheless, always expect the unexpected. When we set off on our journey to the supply vessel's discharge terminal, I had a mental image of large oil storage tanks, bund walls, high fences and neat administration buildings. By the time we'd traveled along 100 or so kilometers of dirt road, I began to think it may not be quite pristine… The truth was like something out of an adventure novel.

As we came round the last bend in the road, we were confronted by a wire fence with large wide-open gates. This was the terminal; quite literally at the end of the road, and backing onto the river. To one side was a native village, complete with rough concrete blockhouses and a few shacks of mud and branches; this was where the workers lived - along with some fishermen and subsistence farmers. My first thought, before getting out of the car, was that the terminal fence could hardly serve any purpose other than marking the boundary between terminal and village.
The terminal manager lived in a single-storey house in the compound, overlooking the river. This Ernest Hemmingway look-alike had spent about ten years living here in splendid isolation, apart from the crocodiles which came up from the river each night, with a trip home to France every month or so. It was little wonder that he was still in his jockey shorts when we arrived, at 09:30. His domain comprised three small tanks (each holding about enough to fill a couple of road tankers), a workshop and the quayside - at which languished the vessel we had examined in PG a few days ago. The security and safety issues at the site were enough to make any self-respecting risk manager have apoplexy but, while making these discoveries, I couldn't help but wonder at the incongruity of it all. A glossy modern ship alongside a dirt quay in a jungle clearing, discharging all kinds of tools, vehicles, equipment and diesel oil - while native fishermen were going about their business in dugout canoes from the adjoining riverbank.

After a few days of this sort of experience, working on high technology installations in Stone Age surroundings and sending nightly reports from my laptop, direct to London, we set off for the drilling camp about 150 miles further inland. Once again, the head office insistence on secrecy was shown to be completely unrealistic, as René and I waited at the airstrip for the only flight of the day to the camp. Even the baggage handlers knew all our names and our itinerary!

A 20-minute flight brought us to a landing strip cut out of virgin forest - and the best passenger security I've seen at any airport, bar none. The difference was, this was directed at incoming passengers! With the smell of oil pervading everything, it wasn't difficult to see the reason; the slightest spark could cause a catastrophe, so security was directed at both the travelers' baggage and their reason for visiting. We were all even issued with a 'visa' which was to be scrutinized several times as we moved around the oilfield.

We lived and worked alongside the resident crews, in basic but comfortable sleeping accommodation and eating at the 24/7 diner. Bowls of coffee with hot croissants for breakfast were *de rigueur*, as this was a former French colony - and the local cooks and workers jealously preserved their heritage. This also meant that all the catering was in the same vein - and the meal breaks were French style, too: lunch wasn't just a snack, to be eaten on the run. It was a full meal, to be savored during a full hour's rest. Dinner was typically French, with several courses, preceded and followed by short - but leisurely - sessions in the bar. Woe betide anyone who over-indulged, though; there was zero-tolerance of even the slightest inebriation, with offenders having their contracts terminated immediately and being put on the next flight home. At their pay rates, no other enforcement was necessary!

The work here was just as challenging as the other sites. The survey of a jungle gas station included damage to fences and equipment caused by marauding elephants. The underlying philosophy was that nothing would stop production, so corners were continually being cut, and all record-keeping was viewed as unwelcome bureaucracy.

There is a constant battle between oilmen and government officials, over dollars and environmental issues, with remote jungle villagers being the pawns. This leads to the oilmen bending over backwards not to disturb the villagers' way of life, while being hounded by regional officials to pay for damage to the environment. The rights and wrongs are not an issue here. Suffice to say, it's rather difficult to run a safe and efficient terminal for barges (transferring diesel from the PG vessel to the drill site tanks) when villagers are free to roam around the unfenced riverbank terminal while children play on the valve gear and pipelines!

We came out of the oilfield by the surface route. This involved joining an escorted convoy of tanker trucks for the three and a half hour drive to another riverside jetty, for the 30-mile trip by boat to the relative civilization of the main compound at the crude oil terminal and tank farm. Even that journey wasn't without incident. About 30 minutes out of the camp, we were stopped by armed security guards who demanded not only the oilfield 'visa', but my 'permit to leave'! This requirement was news even to René and our driver, but the guard was not in a mood to discuss it. The return trip to obtain a permit from the camp added another hour to our journey, while the rest of the convoy waited with the guards at their checkpoint.

After completing the task and presenting my report to local senior management, I was invited out to dinner by René, who wanted me to experience his favorite restaurant. It would of course have been impolite to refuse, so I enthusiastically accepted. I wouldn't even have known the building was a restaurant if he hadn't taken me there and, to be honest, I'd have driven past in the darkness, fearing mugging or ambush. It was little more than a small house with tables outside on the porch and a small cocktail bar to one side. The only other customer looked as if he'd been propping up the bar and drinking the local brew since soon after breakfast, but at least he was quiet. The *patron's* welcome was warm and the beer was cold, so that was a good start. Service was unrefined, but sincere, and the food? Crocodile with manioc doesn't come high on my list of favorite dishes, but it was edible… and interesting! Followed by ice-cream (I still wonder how many times it had been re-frozen) and several beers, finishing the main course soon became my greatest achievement in the eyes of locals and expats alike. Apparently I was the first visitor to attempt it, let alone eat it!

Returning to Libreville the next day with a couple of expats rotating home for their month's leave, I briefed the CEO and CFO on my findings, then had a couple of hours to kill while awaiting the Paris flight. A short tour of the city was a good reminder of the differences between our comfortable western lifestyles and the reality of equatorial Africa. Modern office buildings stand alongside burnt-out shells ("Oh that was when the locals didn't like the way the election campaign was shaping up a couple of years ago - so they torched that hotel…"). Classy French restaurants are tucked away behind dilapidated facades. A handful of well-worn ocean-going sailboats bob in the harbor, together with a naval gunboat which could do with a good coat of paint and a generous dose of TLC, plus a few timber fishing vessels. Everywhere there are groups of people waiting on street corners for the ubiquitous minibus taxis, while the occasional European zips by in a BMW, Mercedes or Jeep.

The result of the project? There were issues besides those I've mentioned, but they are best left between me and the client. Solutions were devised and the project was a success.

In projects like this, in far-flung places way off the tourist trail, it would be easy to forget the brief when surrounded by such a feast of experiences, but these trips are expensive - so the client has great expectations. This translates into the reality that, while the local 'color' provides enough surprises and obstacles to keep you fully occupied, concentration on the task in hand must be absolute and, when a trip lasts ten days, the client wants to see the results of ten days' work. So, the days are long and the pressure intense, but the experiences and memories are priceless.

Some Useful Websites

PI Blogs:

http://investigatornews.blogspot.com/
http://www.pibuzz.com/

This 1997 Investigators' Guide to Sources of Information is published as a service to the investigative community by GAO's Office of Special Investigations. It is intended to be a useful investigative tool for identifying sources of information about people, property, business, and finance. (PDF 117pages)

http://www.gao.gov/special.pubs/soi.htm

AWESOME SEARCH SITE THAT BREAKS INFO INTO CATEGORIES:

http://vivisimo.com/

Donor Lookup: Political Contributions:
http://www.opensecrets.org/indivs/index.asp

This database contains millions of records, so you'll want to narrow your search.

More Political Contributions sites:

http://www.publicintegrity.org/527/db.aspx?act=main

http://cspan.politicalmoneyline.com/index1.html

http://www.opensecrets.org/states/index.asp

http://www.tray.com/cgi-win/indexhtml.exe?MBF=NAME

Corporate Affiliations / Financial Status:

www.theyrule.net

http://www.annualreportservice.com/

http://www.prars.com/ (will mail free annual financial report to you)

http://www.thomasnet.com/ (search by corporation name, product or brand)

http://www.bpn.gov/bincs/begin_search.asp

Who Is Suing Whom (Patent, Trademark and Copyright Edition)

http://www.tlc-i.com/texis/tmp/litcases3

Reunion.com
http://www.reunion.com/showRegistration.do

Federal Inmate Locator:
http://www.bop.gov/inmate_locator/index.jsp

Birthday Database: (birthdatabase.com)
http://217.160.240.239/cgi-bin/query.pl

Death Index:
http://ssdi.genealogy.rootsweb.com/cgi-bin/ssdi.cgi

News – Articles:
http://www.virtualgumshoe.com/resources/index.asp?STATE_ID=&CATEGORY_ID=47

www.factiva.com
www.thelocalpapers.com

Invisible web resource page (HUGE)
http://www.freepint.com/gary/direct.htm

Real Estate: Nationwide
http://homepage.mac.com/researchventures/
www.zillow.com

Great Resource Site:

www.melissadata.com

www.skiptools.com

Motor Vehicle Info:

www.locateplus.com

www.softechinternational.com

Find a County:

http://www.naco.org/Template.cfm?Section=Find_a_County&Template=/cffiles/counties/usamap.cfm

Government Gateway:

http://www.capitolimpact.com/gw/