



THE PALI INFORMANT

Fall 2012

2012 ANNUAL CONFERENCE Special Issue



In this issue

Page 1: Note from the Editor

Page 2: Shifting the Blame to Obtain an Admission

Page 5: Workplace Violence: Early Warning Signs

Page 7: Identifying a Credit Card Issuer

Page 9: Securing Security Compliance

Page 11: Helping PALI, the Environment, and Yourself

Articles by Conference presenters are in bold.

This issue of the *PALI Informant* is a very important one! We've filled it with information about the PALI Annual Seminar, and featured articles by some of the speakers who will be presenting at the Seminar.

We hope that you will join us at the Park Inn by Radisson, in Mechanicsburg, PA right outside Harrisburg, on October 10 and 11. There will also be a great pre-seminar training event featuring Michelle Stuart on October 9.

To register, go to the conference page on the newly remodeled PALI web site at <http://www.pali.org/2012-conference/>. There, you will find everything you need to register for the conference and you'll be able to link from there to make your reservations at the hotel.

You'll get great information, great accommodations, and and have a great time for a very reasonable price. I look forward to seeing you there!

—Bill Everman, *PALI Informant* Editor

PALI BOARD OF DIRECTORS

President

Jeffrey Stein

Chairman of the Board

Richard C. Payton, Jr.

Chairman Emeritus

Robert Meinert

First Vice President

William Everman

Second Vice President

Robert T. Kozura

Secretary

Barbara W. Thompson

Legal Counsel: James West, Esq.

Executive Secretary: Lindsay Kowalski

Regional Directors:

R1: Rick Anderson

R2: Donald "Mac" MacConnell

R3: Charles "Chuck" Kleber

R4: Harry Van Vliet

R5: Ed Linton

R6: Dennis Lagan

Regional Directors At Large:

East (Regions 1 & 2)

Gregory Pirnik

Central (Regions 3 & 4)

Kim Emes

West (Regions 5 & 6)

Christopher Finley

Any questions, suggestions or submissions for this newsletter may be addressed to its editor, Bill Everman, by e-mail to wheverman@comcast.net, by telephone at 610-494-0635, or by mail to PO Box 2006, Aston, PA 19014. Many thanks to Greg Pirnik for his help in editing, and to former newsletter committee members Barbara Thompson and Bob Kozura for their invaluable assistance.

Shifting the Blame to Obtain an Admission

by Robert "Jerry" DeFatta, CFE, CRT

The concept that lying is wrong is instilled in most of us at an early age. As an investigator, it is important to understand that when we ask a person to confess to a crime, we are asking a great deal of that person. To compound the problem, in most cases the interviewee does not know or trust the investigator. Add the fact that the person has most likely already lied to someone else about committing the crime, and it becomes clear that the investigator is in an uphill battle from the start of the investigation.

One technique that can be helpful in obtaining an admission is to assist the person in shifting the blame away from himself or herself and onto someone else. The concept of shifting the blame is also instilled in most of us at a young age. I remember that on more than one occasion, when asked by my mother why I had done something I knew I should not have done, my response was that "everyone else was doing it." This simple response was my way of shifting the blame for my actions to others involved. In the 1970's there was a popular bumper sticker that read, "The Devil Made Me Do It," which leads me to believe that shifting the blame is not a new concept. In this article we will discuss a few of the legally admissible techniques you can use to help suspects morally shift their blame away from themselves. We will also cover some of the pitfalls that you will want to avoid while conducting your admission-seeking interview or interrogation.

Although an admission-seeking interview is not a part of every investigation, the investigator should approach each case with the assumption that one will be conducted. Throughout your investigation you will learn information that will prove valuable during the admission-seeking interview.

When conducting internal theft and property crime investigations, it is helpful to remember and understand the classic criminology theory of the Fraud Triangle developed by Dr. Donald R. Cressey in his work *Other People's Money*, published in 1973. This well-known theory was developed in the 1940s and is still relevant today. The basic principle of the Fraud Triangle is that in almost every case of asset misappropriation, there exist three elements: the opportunity to commit the crime, a pressure that motivates the criminal, and a means of self-rationalizing his/her actions. Identifying each of the

(Continued from page 2)

elements within your investigation will greatly assist you while conducting your admission-seeking interview. That information will better prepare you in developing themes and strategies that you will use during this aspect of your investigation.

By determining how the crime was committed and identifying the source of the opportunity, you may be able to morally shift the blame away from the suspect during the interrogation. In doing this, you will make it easier for the suspect to confess by blaming the source for creating the opportunity that lead to the suspect's acting on the temptation. It is important to remember that you want to morally shift the blame--not legally justify the suspect's actions. The following case will help illustrate this technique:

A convenience store cashier was working the day shift along with her manager. The manager was busy most of the morning in the office counting the previous shift's receipts and making up the deposits. At one point the manager left the store to run a personal errand and left the cashier working alone. While walking to the stock room to retrieve a needed item, the cashier noticed that the manager had left the office door unlocked and partly open. As the cashier reached to close the door she looked inside and noticed the manager had also left the safe open with the deposits visible. The cashier then entered the office and took \$300.00 in cash from the safe. When the cashier was identified as a suspect, an admission-seeking interview was conducted. During the initial phase of the interview the cashier repeatedly denied taking the money. At this point, the investigator began shifting the blame to the manager by stating that the manager's careless act of leaving the safe and office unlocked had created the temptation that ultimately lead to the cashier "acting out of character". It was suggested to the employee that without that temptation, she would have never committed the crime. By shifting the blame to the manager the investigator allowed the cashier to rationalize her actions to herself. The employee confessed, saying that she only went to the office door to close it and that when she saw all the money unsecured she just wanted to teach the manager a lesson.

In another case you might blame the lack of, or failure to enforce, proper internal controls and procedures for making it too easy for the employee to steal. In this type of case you would place the emphasis on others who did not perform their jobs properly.

The pressure or motivation that leads to a person committing a theft can be used in the same manner to shift the blame away from the suspect. As you investigate the crime, you will identify people who had access and the opportunity to commit the crime. As the investigation progresses you will also start to learn more about those people. As you do, you may learn of financial pressures or other circumstances that could have motivated a person to commit the act under investigation. It is important to remember that people react to stress and pressure in different ways. What seems like an anthill to one person might be a mountain to another. Some people will resist temptation at all cost, while others seem to give in to the slightest pressure. These pressures are not always in the form of financial problems or hardships. Pride, peer pressure, and the fear of being viewed, as a failure can be just as great a motivator. If you are able to identify the pressure that motivated your suspect, this too can be used to shift the blame during the interview. By pointing out this pressure and suggesting that the suspect would not have committed the crime had he or she not been under this pressure, you are shifting the blame to the pressure itself. It then becomes easier for the suspect to rationalize his/her actions and feel that others would have acted in the same manner. A good example of this might be a single mother who has stolen money to buy something nice for her

(Continued on page 4)

(Continued from page 3)

child. This fact does not legally justify or excuse her crime, but when contrasted to someone who is stealing to buy drugs, the mother's actions are easier to morally rationalize.

In cases where you are able to deduce how a person rationalized their crime to themselves, this same approach will be affective. In most cases where an otherwise rational person has committed a crime; they have found a way to rationalize their actions to themselves. These self-rationalizations might involve the opportunity or pressure associated to the crime. In one example, if a person felt that if the victim really needed the money, he/she would not have left it unsecured. The victim might be blamed for leaving the money unsecured or for just having more money than he/she needed. The self-rationalization could come from other sources as well. An employee who feels underpaid might rationalize that the company owes him/her what was taken. Revenge is another form of rationalization. If a person feels unfairly treated, that person might rationalize those actions by saying that the victim's actions caused him/her to commit the crime.

In cases with more than one suspect, an effective technique is to shift the blame to the others involved in the crime. This method of playing one suspect against the other is often very effective in cases where the suspects have short term or casual relationships. The investigator can suggest that it was the other suspect's idea or that peer pressure caused the suspect to act out of character. When employees act in collusion with non-employees to steal from a company, this technique is often very effective. When interviewing the non-employee it is easy to shift the blame to the employee, because without access and an understanding of how the company operates, in most cases the crime could not happen. Similarly, when interviewing the employee the blame can be shifted to the non-employee because without their assistance the employee could not have accomplished the crime.

It is important to remember that you do not always have to have another person on whom to shift the blame. The object of the blame could be an entity or a circumstance. You might want to suggest that the blame lies on a company or even on society at large. It would be easy for someone to understand how a poor economy and high cost of fuel could be blamed for causing someone to steal to help support a family.

The most important aspect of this technique to remember is that you are only morally shifting the blame, not legally justifying the crime. As with any other legally admissible interrogation technique, you must avoid using any approach that might cause an innocent person to confess to a crime he/she did not commit. There are many other techniques that can be used, depending upon the situation and the circumstances surrounding the crime. When using any technique, the investigator must be flexible and able to adjust. What appeals to some might not work on others. It might be necessary to try shifting the blame in more than one direction to find the one in which the suspect feels comfortable. The key is to be prepared and to have alternative themes and strategies. The technique of shifting the blame can be used in almost any type of investigation. By understanding the basic criminology theories and learning as much about the crime and suspect as possible, you can greatly improve the chances that the guilty suspect will confess.

Robert "Jerry" DeFatta, CFE, CRT *is the owner of DeFatta & Associates, LLC, a full service private investigative firm located in north Louisiana. Jerry has been licensed as a Private Investigator since 1997 and specializes in internal fraud cases. Jerry conducts training on fraud prevention and investigative techniques. He is also available for speaking engagements. He can be contacted through his web page at www.DeFattaPI.com.*

Workplace Violence: Early Warning Signs

Reginald J. Montgomery, CPP, CLI, CFE, PSP, CST, CP, BCPI, CII, PPS

An average day in corporate America includes 16,400 threats, 723 assaults and 43,800 harassment incidents among co-workers. Over the course of a year, more than 1,000 U.S. workers become homicide victims, while one in four full-time workers are harassed, threatened or attacked. Homicide accounts for 17% of all occupational fatalities and is the leading cause of occupational fatality for women, accounting for 40% of all female deaths in the workplace. Aside from the 36 billion dollars it costs American business, workplace violence affects the lives of thousands of innocent Americans each year. No wonder it tops the concerns list of business executives today.

The motivation toward violence may be greater today than ever before as well. We are a culture steeped in violence, a society burdened with enormous economic pressures. The threat of corporate downsizing, restructuring or lay-off looms over many, some of whom abandon traditional values and choose instead to accept less personal responsibility while expecting more from employers or government. People are afraid and angry, and the sanctity of the workplace is challenged as a result.

Unlike crimes where motivation can be difficult to understand, workplace aggressors can usually be classified in one of six motivational categories. The **Economic** aggressor believes the target is responsible for undesirable economic conditions affecting him, his family or a particular group. The **Ideological** aggressor believes the target is imperiling principles the attacker considers extremely important. The **Personal** aggressor feels inappropriate rage, hate, revenge, jealousy or love. The **Psychological** aggressor is mentally deranged or clinically psychotic, a condition often exacerbated by drugs or alcohol. The **Revolutionary** aggressor obsessively desires to further political beliefs at any cost, while the **Mercenary** aggressor is motivated by opportunity for financial gain.

Workplace aggressors also tend to share common characteristics. They've been influenced by someone or something beyond their control but believe they have suffered a traumatic, insoluble experience and project blame for that experience onto others. They relate poorly, have difficulty getting along with others, and often already have a history of domestic, public or workplace-related violence. Most are male, 35 or older and considered a loner, have few interests outside of work and are at least familiar with weapons. Their self-esteem depends heavily on their job while believing they or their personal beliefs have been victimized by an injustice. Many have served in the military and have a history of substance or alcohol abuse.

Behavioral changes are often the earliest warning signs, including inappropriate emotional outbursts with intense mood swings, overreaction to criticism and unusual paranoia with inappropriate statements or comments. There may be rambling, incoherent speech while isolating from others or an uncontrollable romantic obsession. We see distorted values, exaggerated self-importance and over exaggerating their own value to the organization while devaluing others. In extreme cases the aggressor may demonstrate reckless impulsiveness and destructiveness with an obsessive-compulsive and volatile, sociopathic personality.

Aggressors generally exhibit several of these behaviors over time, displaying a progression toward violence as the behavior becomes increasingly inappropriate. This 'ramping up' progression consists of three phases, each more destructive than the previous. PHASE ONE includes refusal to cooperate with supervisors, spreading harmful rumors, causing disruptions, being argumentative, resisting compromise and seeming to enjoy being disruptive. The aggressor may act belligerent toward customers or clients and often uses inappropriate language or makes inappropriate comments and gestures.

At PHASE TWO the aggressor becomes increasingly argumentative and refuses to obey policies and procedures while repeatedly probing boundaries. He or she engages in subversive or manipulative behavior or sends inappropri-

(Continued on page 6)

(Continued from page 5)

ate messages to co-workers or management while expressing repeated claims of victimization or mistreatment. Some even articulate a desire to harm themselves or others while communicating non-verbal or veiled threats.

In PHASE THREE the aggressor sabotages or vandalizes company equipment or private property, or steals property for revenge, threatens suicide or makes references to the after-life. They become physically aggressive or abusive and threaten physical violence, or commit an assault or some other violent crime. Once in motion, rarely does this progression reverse without intervention. Employers must recognize inappropriate and disruptive behaviors and interrupt the progression before it's too late.

Employers have both a moral duty and a legal obligation to provide a safe work environment, as well as a responsibility to the public, which exposes them to vicarious or direct liable for harm brought to others by workplace violence. Strong policies, effective security protocols, and a well-planned strategy are necessary to mitigate potentially violent employees. The web of statutes, standards, rules and regulations create a legal minefield for management, who must balance these responsibilities without infringing on anyone's rights.

The first step for employers is often to overcome the tendency for denial. Supervisors and managers may deny an employee is a problem, even in the face of irrefutable proof, but in doing so they also deny the employee help. Companies engage in denial by failing to create sound policies or by not enforcing policies already in place. By failing to promptly respond to incidents suggesting the potential for violence, employers unwittingly participate in the progression toward violence. Supervisors and managers must be trained to recognize the danger, and must act on that training appropriately and quickly.

“Employers have both a moral duty and a legal obligation to provide a safe work environment”

When initiated early enough, a well-planned and executed intervention process returns at risk employees to a structured work environment, helping them regain control of their life. Management must act immediately and appropriately, putting the employee on notice with verbal and written warnings, EAP referral and performance monitoring. Extreme cases may call for termination, temporary restraining orders, hospitalization or prosecution.

A threat management team should be formed consisting of executive management, human resources, security and executive protection, legal counsel, public law enforcement, clinical psychology or psychiatry, and private investigation personnel. Crisis management for these incidents will form preliminary objectives based on interviews with the target, witnesses, co-workers, supervisors, former employers and family members, plus a professional background investigation including criminal, civil and driving history, default notices, liens and judgments, bankruptcies, ownership or registration of weapons, personnel files, physicians and law enforcement. Legal counsel should be consulted during this information gathering process to ensure proper balance between the employers right to manage and the employee's privacy.

A workable strategy begins with the incident management team assessment, which forms a basis for dealing with the aggressor. The strategy should redefine performance and behavioral boundaries for the aggressor as well as a tolerance threshold for management. A thorough and comprehensive investigation of both the aggressor and the allegations must be accomplished. The aggressor should be professionally assessed to determine the potential for violence. A best course of action is decided given all available information. Options may include disciplinary or corrective action, referral to EAP, discharge, hospitalization or prosecution. The management team must do all that is practical to achieve the desired result without provoking violence.

Coordination with local law enforcement may not be enough. Safety and security precautions must be implemented, making sure to protect people before property. A solid plan is one that has been reviewed, rehearsed and refined, and includes contingency plans. A review of legal implications and potential liability should be included. The incident

(Continued on page 7)

(Continued from page 6)

management team must communicate with the intended target and meet face-to-face with the aggressor to disclose the actions intended by management. An employee communication session should be frank but respectful of everyone. Legal action should be taken when appropriate, and professional counseling should be provided. A good safety plan means planning ahead to prepare for the unexpected. Employees, clients and customers must be treated with respect and dignity while remaining aware of strangers and their surroundings.

Inappropriate behaviors and activities must be reported and addressed. The way we approach and engage a workplace aggressor can be the key to preventing further incident. It's best to remain calm, slow down and speak clearly while lowering your voice, and, above all, avoid arguing or making threats. It is never advisable to place hands on the aggressor or initiate physical contact if avoidable. A barrier such as a desk should be used to create space between oneself and the aggressor and help should be summoned immediately.

Management must also enforce company policies fairly and consistently, allowing employee complaints and grievances to be heard. Remember, aggressors usually believe they've been wronged in some way. Management must provide the opportunity to resolve problems by nonviolent means. Every employee must understand that violence or threats of violence will not be tolerated and policy violations may result in immediate termination and prosecution.

Workplace aggressors are responsible for their own actions, however management dictates whether the workplace is at risk for violence or not. It is critical for managers to treat all people with respect and dignity and listen to those seeking help. They must recognize and document inappropriate behaviors while properly enforcing company policies and keeping human resources informed. First line supervisors need to de-escalate tense situations if possible and retreat to safety when necessary, and ***never*** hesitate to call for help. A properly trained and prepared Security Professional can save an employer millions of dollars and, more importantly, save life itself.

Employees are always our biggest asset!!

Reginald J. Montgomery is President of [*R.J. Montgomery Associates*](#) in Saddle River, New Jersey, specializing in corporate asset protection and criminal defense investigations with almost 40 years of related experience. Reginald has an extensive expertise in the security and investigations fields. He is a certified polygraphist, protection professional, physical security professional, legal investigator, fraud examiner, security trainer, international investigator, Board Certified Professional Investigator and Personal Protection Specialist.

Reggie has served as vice-chair for ASIS International's Standing Investigations Council and as the chairman of the Northern New Jersey Chapter. He is a life member and past assistant national director for the National Association of Legal Investigators, a life member of the Association of Certified Fraud Examiners and the World Association of Detectives, currently serves on the Board of Directors of Intellenet and is a past Board Member and 3^d Vice President for the Council of International Investigators. Reggie also served as president of New Jersey Licensed Private Investigators Association from June 1996 to June 2000, and has been named to the Certification Board of The United States Association of Professional Investigators. Reggie is an adjunct professor at New Jersey City University. Reggie was named as the National Association of investigative Specialists SPEAKER OF THE YEAR FOR 2006-2007. He has given hundreds of speeches to national and international associations on a number of investigative subjects ranging from product diversion and protecting intellectual property to workplace violence investigations. He is best known for his interview and polygraph workshops.

Reggie has been certified by numerous courts as an expert in virtually every aspect of criminal defense, corporate security and investigative related matters. Reggie has appeared on dozens of network television programs as a polygraph and investigative expert. Mr. Montgomery is the Editor of (as well as contributing author, two chapters) "Corporate Investigations" and contributing author to "Advanced Forensic Criminal Defense Investigations", "Basic Private Investigations" and Advanced Private Investigations".

Reggie can be contacted at: reggie@njinvestigator.com.

Identifying a Credit Card Issuer

by Michele Stuart

During the past several years I have written articles in reference to online research utilizing open sources. These types of open sources can also assist you in some financial research. I have been asked in the past if there is a way to determine what bank has issued a credit card. Understanding that there is an actual rhyme and reason behind the number is the first step. The numbers assigned to credit card are not random. A numbering system called the ISO 7812, through the International Organization for Standardization, oversees the issuing of numbers as well as the magnetic stripe cards. Card Benefit defines a card as 'broken down' by a credit card number, issuer identification number, an account number and a single digit check number used for fraud prevention.

The following site can provide you information regarding issuing banks of credit card, as well as well as identifying bank accounts across national borders. The site explains its capabilities as follows:

Bin Database: Credit Card Bin Checker (<http://www.bindb.com/bin-database.html>)

"The Bank Identification Number, also known as the credit card bin can tell you the name of the bank that issued the card, the type of card like Debit or Credit, brand of card Visa, MasterCard and level of card like Electron, Classic and Gold. From the bindatabase you can also check other details about the card and issuer. Credit card bin numbers are the first 6 digits of a card number. Please note that free credit card bin database checker is connected to Premium Database."

IBAN Generator and IBAN Checker (<http://www.bindb.com/iban-generator.html>)

"This tool allows you to check IBAN for validity. The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders with a minimal of risk of propagating transcription errors. With the iban checker, you can easy validate any country specific format. This IBAN Checker can check IBAN that originates from a member or joining country of the EU or the EEA, plus Switzerland and other countries that have adopted the use of IBAN. A full list of countries is located further down the page. Please note the IBAN Checker: cannot be used to guarantee that an account exists, or that the IBAN belongs to your beneficiary."

Wikipedia (yes, Wikipedia!) has a very useful breakdown listing the numbers and issuing banks that you need to utilize in assisting the identification of a carrier: http://en.wikipedia.org/wiki/List_of_Issuer_Identification_Numbers

Good luck, and happy hunting!

Michele Stuart is a licensed Private Investigator in the State of Arizona with twenty years of experience specializing in the areas of Financial, Open Source Investigations (OSINT), Corporate Investigations, and Intelligence/Counter Intelligence. She started her investigative career as an Economic Fraud Investigator.

Ms. Stuart is an Adjunct Professor with University of Virginia and an Instructor at Quantico for multi country training programs. She provides seminars on her specialized investigative techniques in Open Source Investigations (OSINT). Over the past years she has provided presentations, and private training, to both Federal and State levels of Law Enforcement Agencies and Military Intelligence throughout the United States including attendees of Department of Homeland Security, US Marshals, FBI, DOJ, Border Patrol, Indian Tribal Nations and local law enforcement agencies throughout the country. Additionally, she has presented classes for RSIG, ARA, Allied Finance Adjusters, Insurance Special Investigative Units and numerous financial and state associations. Moreover, she has written and published several articles pertaining to her investigative methods in various investigative publications and journals and is a PI Magazine columnist.

Securing Security Compliance

by William F. Blake, CPP, CFE

Security policies and procedures do not protect individuals or property! Anyone who has conducted a risk assessment of a facility realizes that the average employee does not understand or care about corporate security policies and procedures. Apathy and lack of understanding toward security is very common at all levels of a corporation. Apathy and ignorance are not limited to the employees—management suffers from the same conditions. Employee attitudes are formed by management attitudes and apathy. When managers do not care, why should the employees?

Other problems cause ignorance of safety and security issues. One of the major problems is management's belief that it knows everything worth knowing. Many managers are totally ignorant of the security risks affecting their organization. They only become concerned when they are required to respond to a situation involving death or injury to an individual or one that reflects adversely on the corporate reputation. At that point, the pointing of fingers and the placing of blame is the corporate strategy to place management in the best light possible and put the blame on subordinates. This is nothing more than the abrogation of their management and supervisory responsibilities. Basically it is "pass the buck, pass the blame, and accept no responsibility."

One of the major problems causing management apathy is that security personnel do not require that security policies and procedures be approved at management level. This requirement for management approval creates a situation where management becomes aware of security risks and the actions necessary to implement mitigation actions. Management approval also sends a message to others that security is a management concern and that employee compliance is required. This management approval can not be a "rubber-stamp" action—they must understand the underlying problems and agree that the preventative actions are appropriate.

Security policies and procedures cannot be static documents. Periodic review and analysis should be conducted at least annually. All policies and procedures should reflect the current situation and not be automatically updated without a current assessment of risks.

The most important aspect of obtaining compliance with policies and procedures is ensuring employee "buy-in". When employees believe that the policies and procedures are important, the degree of voluntary compliance will increase. Additionally, management "buy-in" is a necessary ingredient to a successful security program. How to get "buy-in" is not a difficult process.

"Buy-in" can be easily obtained by addressing a questionnaire to all staff members to get their opinions on security risks and preventive measures. Staff members may have identified a security risk but for reasons known only to them, have not brought it to the attention of management or those individuals specifically responsible for the security program. The theft of property from offices or feeling of insecurity when traveling to the parking lot are just two examples of security risks not normally passed on to management. The reasons for non-reporting may be that the individual does not believe that it is a significant risk worth reporting, the fear of retribution, the belief that nothing will be done, or that they will be laughed at by others who do not agree with their perception of a problem.

(Continued on page 10)

(Continued from page 9)

A security suggestion program in concert with a reward program will stimulate employee participation and compliance with the security program.

Another method for obtaining “buy-in” is employee involvement in developing the policies and procedures. When employees feel that they can have input into something that affects them, they will be more apt to comply with the program. As part of developing appropriate security policies and procedures, the employees will provide input on what they consider to be realistic controls, while at the same time providing different perspectives on the impact of the policy or procedures.

To impact compliance, there must be a comprehensive and realistic explanation of the security program and the benefits to the employee and the overall business entity. Standing in front of a group of people and reading the policies and procedures to them is not an effective method of communication. The use of PowerPoint presentations, TV clips and reports of actual incidents will provide a more interesting orientation without putting people to sleep because of boredom. Another significant method is to have a speaker from a business that has suffered a loss due to a security risk who can relate the effects of a good security program from a realistic experience.

To establish credibility and to ensure understanding, policies and procedures must be periodically tested. Failure to do so will significantly increase civil liability in event of a security risk problem. All employees, and all tenants in the case of a multi-tenant building, must be required to participate in testing as required. For example, if there is a policy that requires periodic fire drills, they must be accomplished and all affected personnel must participate without exception.

Obtaining compliance with security policies and procedures is not an easy task but one that can be accomplished with a group effort by employees and management and continuous testing to identify current risks and understanding of desired outcomes.

William F. Blake, the president of *Blake and Associates, Inc.*, is a native of Vermont, and a graduate of Michigan State University, East Lansing, Michigan, with a Bachelor of Science degree in Police Administration. He also holds a Master of Science degree in Foundations of Education from Troy State University, Troy, Alabama.

He is a retired Chief Warrant Officer of the U.S. Army where he served as a Military Intelligence Special Agent and a Criminal Investigation Division Special Agent in supervisory and management positions. Following retirement from the U.S. Army, Mr. Blake was employed as a security officer with a hospital before accepting a position as Security Manager and Investigator for a major bank. Mr. Blake was later employed as a Security Manager for a savings and loan association with state-wide responsibility for 25 locations. From 2000 to 2002, he was President of Prism International, Inc., a security consulting firm with a national and international clientele.

Mr. Blake has more than 45 years experience in civil and criminal investigations, bank security, executive protection, loss prevention, disaster recovery planning, counterintelligence operations, security risk analysis, and security training.

Help PALI, the Environment, and Yourself!

Sign up for the digital edition of the *PALI Informant*

If you haven't already, sign up for the digital version of the *PALI Informant*! The digital edition saves PALI printing and postage costs, helps the environment by reducing the use of paper, and helps you to dig deeper into subjects of interest to you by providing links to relevant web sites and e-mail addresses in articles and advertisements.

To sign up for the digital edition of the *PALI Informant*, simply send an e-mail to PALI's newsletter editor, Bill Everman, at wheverman@comcast.net, with "Informant Online" in your subject line. Your mailing address will be removed from the next newsletter mailing, and the digital version of the *Informant*, in .pdf format, will be sent to your e-mail address.

You do not need to be a PALI member in order to sign up for the digital edition of the *Informant*.

If you would like to continue to receive the print version of the *Informant*, you don't need to do anything!

STANDARD ADVERTISING RATES

Business card.....	\$30.00
Quarter page.....	\$160.00
Half page.....	\$250.00
Full page.....	\$375.00

Contact Bill Everman at wheverman@comcast.net, or
at 610-494-0635.

Limited design assistance is available. Ask about adding a link to your web site or e-mail to the digital version of your ad!

Help This Newsletter, And Your Business, To Grow!

While this issue, focusing on the upcoming Conference, is advertisement-free, our first few issues have seen great support from PALI members. We'd love to hear from you if you're interested in writing for or advertising in our newsletter, but there's another way you can help, and earn a free business card ad for your efforts.

If you know a client, vendor or other anyone else who offers a product or service that may be of interest to PALI members, talk to them about advertising with us. If they purchase an ad larger than business card size, and mention that you referred them to us, we'll give you a free business card ad. If you have any questions, just call Bill Everman at 610-494-0635 or email him at wheverman@comcast.net.

**Pennsylvania Association of
Licensed Investigators, Inc.**

P.O. Box 651

Lemont, PA 16851-0651

Telephone:(610) 696 - 7799

Fax:(610) 441 - 7539



Visit us on the Web at:
www.pali.org

**Join us for the
2012 PALI Conference**

October 10-11, 2012

**Pre-conference
Training October 9**

Details inside!