



LAW ENFORCEMENT LIAISON COUNCIL

February 2010



Partners!

LEADERSHIP 2010

Chairperson:
[Ms. Oksana Farber](#)

Vice-Chairperson:
[Mr. Edward Appel](#)

COMMITTEES:
(Chairpersons)

Executive Committee
[Brian Reich, CPP](#)

Annual Seminar
[Mr. Michael D. Gambrell](#)

Book Reviews
[Mr. James Brown](#)

Council Certification
[Mr. Paul Sweeney, CPP](#)

Guidelines Committee
[Mr. Mark Riesinger, CPP.](#)

Membership Committee
[Mr. James W. Birch](#)

Publications Committee
/Newsletter Editor
[Mr. Robert E. Lee, Jr.](#)
Lee_Robert@Cox.net

Session Reviewers
[Mr. Robert F. Graham, CPP](#)

Subject Matter Experts
[Mr. Ira S. Somerson, CPP](#)

School Safety&Security
[Sgt. Michael Scala, CPP](#)

Transitional Training
[Ms. Stacy Irving](#)

Web Master
[Mr. Mark Competello](#)

CONSULT:
"ASIS Dynamics"
for LELC
leadership contact
information.

LELC: OPENING REMARKS

From the Desk of Ed Appel, Vice-Chair LELC

Reflection and Renewal

New Year's is always a time of reflection on the past year, and resolutions for the year to come. The LELC always meets just after the New Year in a comfortable setting near the Nation's Capital to renew its resolve, reflect on its achievements and set new goals.

Among the many achievements and successes of the past year, we celebrated and moved forward on several at the Ritz Carlton, including implementing the MOU between ASIS International and IACP. Although the Associations rarely endorse MOUs, this understanding is really an acknowledgment that the LELC and Private Sector Liaison Committee of IACP will work together, as will the Associations, where it makes sense, and where goals are closely aligned. In the cases of the LELC and PSLC, it's "putting our money where our mouth is," and "ganging up" on problems that both the council and committee have in their sights. Seeing the highest leaders of both Associations' professional officers and executive staff together was uplifting, and their mutual goals and intentions far outweighed any hesitations to work together. Although both have politely co-existed for decades, this renewal of joint intent will have far-reaching impact on two of the most active and effective groups in both associations, as the LELC and PSLC move together on a range of initiatives.

In 2009, the list of LELC activities became too long to recite, without fear of overlooking good work. Nevertheless, it's worth a quick glance back, to see the achievements, including transitional training, Operation Partnership publication, 2010 Terrorism Symposium, new LE-PS partnerships in Florida, Georgia, Colorado, Europol, Interpol, Major City Chiefs, National Sheriff's, etc., National Center for Missing and Exploited Children (NCMEC), Safe Cities, Shanahan Award and recognition dinners. Included should be dozens of presentations by LELC members supporting the principles, processes and goals of LE-PS partnerships nationwide, and abroad. We have never really stopped to count the number of instances in which LELC members and their associates have had a local, regional, national and international impact on police-security collaboration, but in 2009 it was significant. Even the bookstore reflected LELC members' impact, as Ira Somerson published *Art and Science of Security Risk Assessment*.

In 2010, we not only enter a new decade of a new century, but we plan to take our cause to a new level. Among the efforts underway are further work with fellow

associations, including IACP, NSA, state and city police chiefs, NCMEC, new Safe Cities, police, military and intelligence professionals transitioning to security, new Shanahan Award winners, a cyber vetting project with PERSEREC, renewed interest in school violence and armed security guards, assisting the Bureau of Justice Statistics with a study of private security, starting with security guards, and others too numerous to mention. Key to success will be the efforts of on duty and retired professionals from law enforcement and private security, academia and government, working together to protect us all, locally, regionally, nationally and globally.

The nearly overwhelming weight of a global depression had its impact on the LELC in 2008 and 2009. For some, the drag has continued into 2010, and because of the natural aging process, we have all thought of where we can afford to expend our efforts in the coming months and years. It has never been more important than now to plan together to keep up the strength and achievements of LE-PS partnerships. That's why the LELC has taken the initiative of establishing an Executive Committee to reinforce our strategies and ensure continuity for the future. We should all think about how best to add resilience to the collaboration that we have learned can make the difference between success and failure in policing and private security.

Where the LELC and PSLC see opportunities for funded research (e.g. from government, corporate or foundation-sponsored projects), we should try to include ASIS and IACP as recipients of research funding. In that way, we can strengthen the platforms on which our partnerships depend, through our volunteer labor paired with funding for supporting ASIS and IACP staffs.

We frequently receive expressions of interest from ASIS professionals in the work of the LELC. Recent volunteers have included exemplary practitioners from the military, law enforcement, corporate security and contract security, all eager to help with LE-PS partnerships. The forecast for 2010 and beyond is for a strong LELC, and we welcome our brothers and sisters with the same vision and goals to build this effort into the future.

My number one resolution for the LELC in 2010 is to think of ways to include "all-pro's" from LELC, PSLC and their many associates in all of our activities, to improve the quality of each project and ensure a more rapid and higher-impact success.

Just one last note, looking both backward and forward: Thanks to Oksana Farber for her LELC leadership, friendship and strength in 2009, and a pledge of continued support in 2010.

Lessons Observed, Lessons Learned and Lessons Applied: What Are The Differences And Does It Really Matter?

Tom Conley, LELC member, CEO, The Conley Group

From the beginning of the human race to the current time, human beings have traditionally learned and applied lessons that have enabled us to evolve in a variety of ways. Most of the lessons we have learned and applied are positive, while some have enabled us to evolve in ways that are not so good. Irrespective, here we all are – starting 2010 with many past successes and failures, and a plethora of future threats facing us.

While I am pleased at the successes we had enjoyed, such as stopping more terrorist attacks on our country since 9/11 than the public will ever know about and the progress made with public/private partnerships, I cannot help but ponder why some failures have occurred and what we can do to have fewer failures and more successes.

Whenever an incident or situation occurs, we appropriately tend to dissect that incident or situation to determine what actually occurred, what our response was, if that response was adequate, and what we learned that could help us avert or manage further incidences or situations. Far too often, we fail to properly extract all available information and then properly apply that information to provide us with the maximum opportunity to avert a future adverse incident or situation, or, at minimum, to better manage an adverse incident or situation if it does occur. Never was this clearer to me than our failure to intercept Umar Farouk Abdulmutallab as well as the manner in which this situation was treated once he was captured. Abdulmutallab, also colloquially known as the undie bomber, is an al Qaeda-trained Nigerian man accused of trying to blow up an American passenger jetliner bound for Detroit on Christmas Day 2009.

To understand why we collectively keep repeating mistakes, we need to look at the critical parts of the process that are largely responsible for determining successful as well as unsuccessful outcomes to a variety of situations and circumstances. In order to do this, we need to take a close look at the individual and cumulative aspects of lessons observed, lessons learned and lessons applied.

The term “lesson learned” is a catch-all expression that is commonly used to identify knowledge that has been gained. Traditional lessons learned are typically acquired by incident dissection, learning from others, by reading case studies, after-action reports, results of audits and investigations, and from personal experience. The problem with using the term lessons learned as a catch-all expression is that it leaves out two important steps in the learning process. Those steps are lessons observed and lessons applied.

Most of the time, when we discuss lessons learned I believe we actually mean lessons observed.

A lesson observed can be described as the act or instance of noticing, perceiving and identifying a problem or situation. In the lesson observed stage, decisions are made relative to the importance, or lack thereof, about the value of the problem or the situation identified. A lesson observed only starts to become a lesson learned when a determination has been made that the problem or the situation identified is relevant to a particular outcome. Once it is identified that a lesson learned is necessary, there is then a maturation process that occurs. This maturation process involves research and application of other learned lessons to the lesson observed. Some of the most important factors that provide real learning opportunities come from failures. A lesson observed can only become a lesson learned after this maturation process has been properly completed. However, the only thing that really matters is when a lesson learned becomes a lesson applied.

A lesson applied ONLY occurs when appropriate action is taken that uses the knowledge acquired from a lesson learned to create a positive change. In the absence of a positive change creating a lesson learned, the entire process of a lesson observed becoming a matured lesson learned is literally moot. In fact, it is lessons applied that make the real difference in our ability to help avert future incidences or situations successfully.

With respect to applying the process to the Abdulmutallab situation, our country did not do so well in my opinion. The following is a highly simplified analysis of process relative to the Abdulmutallab matter:

What were the lessons observed?

From the first WTC bombing in 1993 through the USS Cole attack in 1999, it was evident that al Qaeda and other terrorists groups were a clear and present danger to our country.

What were the lessons learned?

The events of September 11, 2001, in conjunction with the prior lessons observed, resulted in an undeniable lesson learned that al Qaeda was at war with us but we were not at war with them. This prompted a fundamental change in our approach to terrorists from us viewing and handling terrorism as a law enforcement matter to us taking a military approach to terrorism.

What was the lesson applied?

That we needed to go on the offense and be at war with our enemies until they are defeated. Among many other actions, this included wide-sweeping changes in the U.S. such as standing up the U.S. Department of Homeland Security, passing the Patriot Act, bolstering our intelligence mechanisms and interrogating enemy combatants – all so we could gain actionable intelligence that would help us prevent future attacks.

If there were lessons observed, lessons learned and lessons applied, then how was it possible for Umar Farouk Abdulmutallab to be able to board an American passenger jetliner and almost kill at least 300 people and then, after being taken into custody, claim to have knowledge of future planned attacks against the United States, but not be fully interrogated by our national intelligence assets? The answer to these questions lie in the failure of our leaders to remember the lessons observed, lessons learned and lessons applied. As an example, one of the lessons learned on 9/11 was that al Qaeda was at war with us but we were not at war with them. The resulting lesson learned was

that we needed to change our approach to terrorists from our viewing terrorism as a law enforcement matter to taking a military approach. Yet, not only was Abdulmutallab allowed to board an American passenger jetliner without detection or interception, but his terrorist attempt is now being treated as a law enforcement matter versus the attempted terrorist attack being handled as him being an enemy combatant.

Does it really matter if we ignore lessons observed, lessons learned and lessons applied? I advocate that it does matter, and that we ignore these lessons at our own peril. As I stated, in the absence of positive change created by a lesson learned, the entire process of a lesson observed becoming a matured lesson learned is literally moot. Once a lesson is applied and works, it is advisable to never forget the background that resulted in why and how that lesson applied came to be initially.

ACTIVE SHOOTER IN YOUR LOBBY: NOW WHAT!!!!

- Article collaboration: Jim Birch, Stacy Irving, Walt Smith, LELC members

Ok, you are a property manager and a deranged individual has entered the lobby of your building and is actively engaged in killing or attempting to kill people without an apparent pattern or motive. **WHAT DO YOU DO???**

This question was put to a group of property managers in Philadelphia at a seminar sponsored by the Philadelphia Center City District [CCD] and the Philadelphia Police Department [PPD]. The CCD, known for being the catalyst in forging partnerships between the public and private sectors, and the PPD, anxious to explain their recent adoption of the Active Shooter Response philosophy, sparked a dialogue that is vitally important in mitigating the loss of life in an Active Shooter situation.

First – some definitions: An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms and there is no pattern or method to their selection of victims. An Active Shooter Police Response is designed to stop the active shooter as soon as possible. Officers, usually in teams of 4, will proceed directly to the area in which the last shots were heard.

The main question from the group of property managers was – “Many office buildings in Center City have their own security presence. **What is the best action for private security to take that can assist the first police officers that arrive on the scene?**”

Before developing a strategy for building security officers, it was felt that **building managers needed more information as to how the Police would actually respond**. With the help of CCD, the Security Director for the Comcast Center [newest high-rise in Philadelphia] and Chief Security Officer for the Comcast Corporation were invited by PPD to participate in the training program given to the city’s police officers. This was followed by an invitation by the Comcast Center security team for police officers assigned to that part of the city to conduct active shooter response drills in the public and tenant areas of the building. These two initiatives provided an appreciation and acknowledgement from both the police and private security of the challenges involved and greatly assisted private security in identifying key components for a building plan.

While an Active Shooter Emergency Action Plan for security will vary from building to building, it became clear that the primary role of building security is to minimize victimization by preventing tenants, visitors, and guests from inadvertently entering the area located by the shooter. **Manual recall of elevators, ‘safe rooms’ within the building, partial or full evacuation and/or shelter-in-place, designated contact for police for building logistics, use of CCTV and access control, are all strategies that can be critical in mitigating the number of injuries.** The best plan is one that takes into account the needs of the police first responders and knowledge/expertise of building security and building management of the building itself.

Inherent in the mission of the Law Enforcement Liaison Council, ASIS International, is the work to foster vital private/public partnerships between law enforcement and private security. The Philadelphia example shows the power of collaboration between the Center City District, Philadelphia Police Department, and the Comcast Center in addressing a difficult issue and identifying a strategy that fits the needs of both the private and public sector. Regardless of the community in which you reside, there are opportunities for this same level of collaboration and success.

Internet Facilitated Identity Theft *Mark Competello, CHS, CPM, CPP, CCE, CFC, LELC* *Member, Lieutenant, City of Hoboken Police Department*

What is Identity Theft?

Traditionally, the term ID Theft has been utilized to describe any use of stolen personal information. According to the U.S. Federal Trade Commission (FTC), approximately 10 million Americans are affected by identity fraud each year due to computer theft, loss of backups, or compromised information systems.

The structure of the Internet, although convenient, remains problematic with regards to ID Theft related crimes and incidents reported by victims. As the technology and vast resources of the Internet continue to improve, unfortunately so do the methods of criminals they prey on consumers. The Internet, because of its accessibility to all, has resulted in a cloak of anonymity to a degree in regards to scammers. Additionally, a person who commits ID Theft has access to virtually a “global” pool of potential victims, via the Internet. Some methods of ID Theft via the Internet are as follows:

Phishing

Perhaps the most commonly used and identified method is phishing. This is a solicitation of information via e-mail, or the culling of individuals to fake Web sites (i.e. those designed to look like a legitimate firm). Such messages usually ask the potential victim to click a “link” and go to that website and update their personal information, or give a credit card number. Many sites are realistic and fool even the savviest consumer. A quick antidote to this scam is to look in the URL address bar of the browser and confirm that legitimate business is in fact that business (i.e. the banks name.com or other). A Phishing Web site will have a “hijacked” address not pointing to the legitimate business claimed. A simple remedy would be DO NOT ever click a link or provide information unless you have knowledge of its legitimacy or simply call the business on the phone.

Spoofing

Spoofing involves E-mails or Web sites using company trademarks and logos that appear legitimate. Such scams use banks and financial institutions to carry out their scam. Pay-Pal is notorious for spoofing.

Pharming

This is an advanced form of Phishing, which redirects the connection between an IP address and its target server. It is accomplished by using a “mirror site” that is altered to fool an unwitting potential victim.

Redirectors

These are malicious programs that redirect user’s network traffic to undesired sites.

Spy ware-Generally

Consumers often precipitate their own victimization by opening file attachments, downloading free software, screensavers, songs, or by downloading video clips or images from adult Web sites. These sites unwittingly affect the person’s PC and installs spy ware. A good anti-spy ware is suggested to combat this malicious activity.

Key loggers

By definition *key loggers* are software programs, which record the input activity of a computer or system via keystrokes. Depending on the device employed, captioned information is stored locally or also is remotely sent to the perpetrator. Key loggers are usually installed in the USB port of a PC that is then directly connected to the keyboard. This device can be detected by the naked eye and removed and examined.

Source: Britz, Masrjie, 2004. *Computer Forensics and Cyber Crime, 2nd Edition*. Prentice Hall: New Jersey

National Private Security Survey (NPSS)

Lynn Langton, BJS & Michael D. Gambrill, LELC member, Dunbar Armored, Inc.

The Bureau of Justice Statistics (BJS) of the U.S. Department of Justice is beginning a comprehensive research project on the Private Security Industry. Few research efforts of this scale have been undertaken since the Hallcrest studies in 1985 and 1990. The lack of national-level data about the private security industry represents a major gap in our country's knowledge of our justice system.

BJS maintains a number of ongoing statistical collections on public law enforcement agencies and officers, including the Census of Law Enforcement Agencies and the Law Enforcement Management and Administrative Statistics (LEMAS) series. As we are all aware, however, collecting data on public police agencies only gets at a proportion of the entities and individuals that provide security services. Estimates suggest that employment in private security is at least three times that in law enforcement, so BJS is missing a big piece of the security picture. BJS has been discussing for several years the possibility of branching out to conduct complimentary data collections on private security as well.

There are many difficulties in collecting data from private security industry versus public law enforcement:

1. No uniform definition of the industry
2. Multiple data collection approaches are likely necessary for each of the segments of the industry
3. Private industries tend to be less willing to participate in survey research

Because the private security industry is complex and because collecting data from private companies is quite different than collecting from public agencies, BJS is currently conducting a design project to explore the possibility of a data collection effort on the private security industry. BJS needs to begin with an initial data collection effort that is manageable, feasible, and can hopefully be built upon in the future

In October 2009, Research Triangle Institute (RTI) was awarded a contract that tasks them with pulling together private security experts, associations, and practitioners, to assist in determining what the scope of a private security data collection project should be (in other words, what sector(s) of the private security industry can BJS feasibly collect useful and reliable information about), what type of sampling frame would allow for making national estimates, what questions and topics BJS should be gathering data on, how they can reach out to the private security industry to get buy-in and participation, etc.. Depending on what is learned from this design effort, the prevailing thought has been that BJS would like to start with a more focused data collection, possibly examining just private security officers, for example, and hopefully with success over time, branch out and expand from there.

The ultimate goal for the NPSS will be to obtain much-needed, comprehensive information on the characteristics of private security professionals, including their prevalence, demographic characteristics, workloads, clients served, selection and training requirements, relationship with public law enforcement agencies, and role in critical infrastructure protection and homeland security. The NPSS data will not only increase the understanding of private security for the general public, legislators, law enforcement agencies, and community planners, it will also provide the security industry with benchmark numbers to use for planning and forecasting purposes.

Any research is only as good as the data collected. It is imperative that the private sector security industry cooperate with this effort to insure that the final report is a good comprehensive examination of the private security in the United States. Please use the below contacts for input into this much needed effort.

Lynn Langton, lynn.langton@usdoj.gov, 202-353-3328

Brian Reaves, Brian.reaves@usdoj.gov, 202-616-3287

Mike Gambrill, , mike.gambrill@dunbararm.com, 410-229-1923

FYI – Shanahan Award

The 2010 application for the Shanahan Award is now available on the IACP Website. The award seeks to recognize outstanding achievement in the development and implementation of public/private cooperation in public safety. This award recognizes agencies who have demonstrated outstanding achievements in cooperative efforts in public safety.

For further information follow this link:

<http://www.theiacp.org/About/Awards/TheMichaelShanahanAward/tabid/98/Default.aspx>

All articles are the opinion of the author(s) and not necessarily that of ASIS International or the LELC.

