



LAW ENFORCEMENT LIAISON COUNCIL

JULY 2009



LEADERSHIP 2009

Chairperson:
Ms. Oksana Farber

Vice-Chairperson:
Mr. Edward Appel

COMMITTEES:
(Chairpersons)

Annual Seminar
Mr. Michael D. Gambrell

Book Reviews
Mr. James T. "Tom"
Roberts, Jr. CPP

Guidelines Committee
Ms. Gail M. Simonton
Esq.

Membership Committee
Mr. James W. Birch

Publications Committee
/Newsletter Editor
Mr. James H. Fetzer, III
CPP: jfa@tds.net

Session Reviewers
Mr. Robert F. Graham,
CPP

Transitional Training
Mr. James Birch, Ms.
Stacy Irving, Mr. Walt
Smith

Web Master
Mr. Mark Competello

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

LELC: OPENING REMARKS

*From the Desk of Oksana Farber, Chairperson LELC, President Trident
Master Executive Development*

Information sharing, as we in the security industry know and respect it, is a combination of reliable knowledge management, appropriate confidentiality and professional engagement. Careful and systematic practices outline how to find/create, organize, share then use/reuse the cycle of knowledge. Absent from these disciplines, chaotic and unverifiable knowledge received from Tehran after the elections via Twitter's free, global connectivity has produced emergent effects and many concerns. Global knowledge, accurate or not, runs on high-octane fuel at hyperspeed reaching every person on the planet on many different devices. What is the human networks' social media role in international security and politics, if any? Homeland Security experts' perceptions are that hyperconnectivity is amplifying capabilities but, so far, there aren't many examples of "open source" social media crossing the public-government security boundary. To enablers of public-government information sharing initiatives, one thing is certain: online information sharing and some data aggregation are in full-blown growth mode. By taking a "wait and see" approach as they study online information-sharing social media capabilities, they recognize that privacy is dead. DHS, ICE, EPA, DoS and other government agencies discussed rapidly developing information-sharing standards, collaborative initiatives and frameworks, all existing in very controlled privacy policies and programs. These privacy policies and security controls are quickly being re-examined. Potent and reliable information-sharing tactics should not become dangerously confused and blurred, heightening this nation's vulnerabilities.

The LELC assists in making a real impact on our nation's security by making deep and lasting improvements to public-private partnerships and seeking opportunities for the creation of new ones, working to confront new threats, helping to ensure business continuity, protect the homeland and offer insights to influence national security policy. Amongst many others, some of the current LELC's projects and activities demonstrate the maneuvers required for the establishment of effective communications: JAMES BROWN coordinated a conference call between the IACP executive director Dan Rosenblatt and BENS director Steve Ewell to help facilitate a dialog that will help BENS to develop a strong law enforcement component; BOB PENCE met with Major City Police Chiefs and Major County Sheriffs in Sun Valley and will report on the Colorado

Chiefs meeting with the ASIS chapter chairman in Springs, CO; GLEN MOWREY reported on the Florida Police Chiefs Association's outstanding teamwork approach that is being used as a model public-private partnership and his LELC presentation at the Raleigh-Durham, NC ASIS chapter; STEVE HARRIS delivered a "Vision of Success" presentation to the Puget Sound, WA ASIS chapter; BRIAN REICH coordinated a meeting at the National Center for Missing and Exploited Children, which entailed discussions about providing response training for missing children incidents to the private sector security executives; BOB GRAHAM and BRIANE GREY are assisting the Global Terrorism & Political Instability Council's coordination of their March 2010 symposium; IRA SOMERSON's book "The Art and Science of Security Risk Assessment" was published by ASIS International; JIM FETZER consistently drives the commitment to document our information-sharing and public-private partnership experiences in this publication, the LELC Newsletter; thanks to AL YOUNG, a PERF executive will be attending the LELC annual meeting in Anaheim at the ASIS Seminar in September; STACY IRVING reported on the transitional training committee's efforts to provide training in October in Philadelphia and again in November in Boston; PAUL SWEENEY and BOB GRAHAM are the "working group" team leaders in a multi-Council initiative to promote the Safe City program; MIKE GAMBRILL, STEVE HARRIS and ED APPEL with our friends and colleagues at the IACP's PSLC composed the original draft of the MOU between the IACP and ASIS, which will be signed by the presidents of both respective organizations; ED APPEL, LELC vice chair is scheduled to present an ASIS Webinar "Mastering Internet Searching & Analysis for Investigations and Security". Additionally, the LELC is sponsoring four sessions at the ASIS Annual Seminar: 1) session #87 "Operation Partnership"; 2) session #139 "Private Security and Missing & Abducted Children Events"; 3) session #140 "LA County Approach to CIP"; and 4) session #142 "Life After the Badge".

We may be in a new age of hyperconnectivity but it is still a very human era, one that, now more than ever before, needs to be able to rely on accurate, timely and trustworthy information that can and should be shared with stakeholders that help to keep our nation safe and secure.

Thanks to all LELC members for your productive teamwork, leadership skills, dedication, drive, integrity and hard work.

"The greatest lesson that I have learned,
the most important part of my education,
is really the essential imperative of this century.
It is called leadership."
Jack Valenti

COMPUTER FORENSIC METHODS in the PUBLIC and PRIVATE SECTORS

Mark Competello, CHS, CPM, CPP, CCE, CFC, LELC Council Member, Lieutenant, City of Hoboken Police Department

What is Computer/Digital Forensics?

What is the role of digital or computer forensic examinations in criminal and civil litigation? Digital (or computer) forensics is the acquisition, examination, and reporting of information found on computers, networks, and other digital devices (e.g., cell phones, I-Pods, Flash media and PDAs) that pertain to a criminal, civil, corporate, other private sector incidents. Nearly everything that someone does on a computer or a network leaves traces -- from deleted files and registry entries to the Internet history cache and automatic Microsoft Word backup files. E-mail headers and instant messaging logs give information as to the intermediate servers through which information has traversed. Server logs provide information about every computer system accessing a Web site.

Digital forensics is increasing in importance in both public and private sector investigations for a number of reasons, not the least of which is that computers and the Internet represent the fastest growing technology tools in human history. Digital devices are increasingly the target, instrument, and/or record-keeper of everyday activities, including those of a criminal nature and/or of interest to a civil investigation.

Why is Computer Forensics Important?

Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a “defense-in-depth” approach to network and computer security. For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.

What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data. Computer forensics is also important because it can save your organization money. Many managers are allocating a greater portion of their information technology budgets for computer and network security.

From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case. Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. The investigator must also pick the appropriate tools to use. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

Types of Digital Evidence

Two basic types of data are collected in computer forensics. *Persistent data* is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off. *Volatile data* is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it. System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

Legal Aspects of Computer Forensics

Anyone overseeing network security must be aware of the legal implications of forensic activity. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion. There are also legal ramifications to using security monitoring tools. Computer forensics is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux.

New court rulings are issued that affect how computer forensics is applied. The best source of information in this area is the United States Department of Justice’s Cyber Crime web site. The site lists recent court cases involving computer forensics and computer crime, and it has guides about how to introduce computer evidence in court and what standards apply. The important point for forensics investigators is that evidence must be collected in a way that is legally admissible in a court case.

Increasingly, laws are being passed that require organizations to safeguard the privacy of personal data. It is becoming necessary to prove that your organization is complying with computer security best practices. If there is an incident that affects critical data, for instance, the organization that has added a computer forensics capability to its arsenal will be able to show that it followed a sound security policy and potentially avoid lawsuits or regulatory audits.

There are three areas of law related to computer security that are important to know about. The first is found in the United States Constitution. The Fourth Amendment allows for protection against unreasonable search and seizure, and the Fifth Amendment allows for protection against self-incrimination. Although the amendments were written before there were problems caused by people misusing computers, the principles in them apply to how computer forensics is practiced.

Second, anyone concerned with computer forensics must know how three U.S. Statutory laws affect them:

- Wiretap Act (18 U.S.C. 2510-22)
- Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
- Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)

Violations of any one of these statutes during the practice of computer forensics could constitute a federal felony punishable by a fine and/or imprisonment. It is always advisable to consult your legal counsel if you are in doubt about the implications of any computer forensics action on behalf of your organization.

Third, the U.S. Federal rules of evidence about hearsay, authentication, reliability, and best evidence must be understood. In the U.S. there are two primary areas of legal governance affecting cyber security actions related to the collection of network data: (1) authority to monitor and collect the data and (2) the admissibility of the collection methods. Of the three areas above, the U.S. Constitution and U.S. Statutory Laws primarily govern the collection process, while the Federal Rules of Evidence deal mostly with admissibility.

If system administrators possess the technical skills and ability to preserve critical information related to a suspected security incident in a forensically sound manner and are aware of the legal issues related to forensics, they will be a great asset to their organization.

The author is a Certified Computer Examiner (CCE) and a Certified Forensic Consultant (CFC) with extensive training and certifications in digital forensics and computer administration, including expert testimony. Additionally, the author performs digital forensics for the private sector with his own business: TMD Computer Forensics, LLC <http://www.tmdcomputerforensics.com/> The website contains information about digital forensics and its many uses.

SECURITY OFFICER DEATHS

Robert E. Lee, Jr. is a member and former chair of the LELC. As Principal Consultant for Mason-Coburn Partners, LLC he provides consulting services surrounding Organizational Change related to Technology. He can be reached at Lee_Robert@cox.net.

Not all who become security professionals have a sense of the dangers of their chosen profession. Stephen Johns may have been one of them. On June 10th he was killed at his job site, the Holocaust Museum in Washington, D.C. He had worked there for six years.

Stephen Tyrone Johns, 39, opened the door for the man authorities say killed him. At 6'6" tall, Johns was described as a care bear that wouldn't hurt anyone. To advance his trade he became sworn as a Special Police Officer (SPO) which allowed him to carry a gun, and thus increased his value to his employer. But his killer got the drop on him and, fortunately for others at the Museum, two other security officers at the Museum returned fire when Johns was shot and neutralized the shooter.

The death of Security Officer Stephen Tyrone Johns pushes forward the risk inherent in protecting people and assets. Despite the best intentions of security planners, when an individual penetrates our preventive tactics and mechanical controls, it turns to the human to intervene. Officer Johns by his willingness to accept the responsibility for his position at the Museum set in motion a series of events that actually saved others because he was part of a team that reacted according to their training.

According to the Washington Post, all of the officers were employees of Wackenhut Services, a large private security firm that provides protection for several government buildings, including the Federal Aviation Administration and the Nuclear Regulatory Commission. At the museum, the guards look just like police

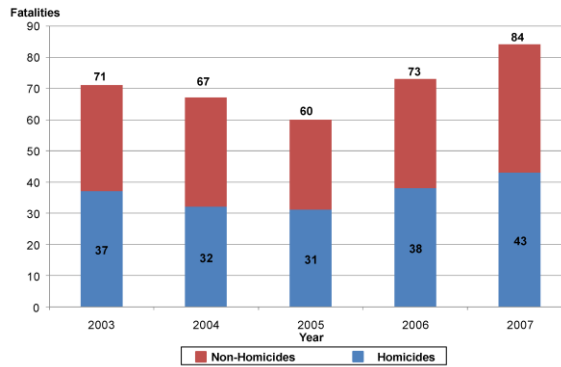
officers, with crisp uniforms, .38-caliber revolvers on their hips and silver badges with an image of a lion on a scale on their chests.

The SPO is different from a regular security guard, who "is a civilian who has no police authority," said D.C. Police Lt. Jon Shelton. SPOs, by contrast, are commissioned by the D.C. police chief and have "full police authority," including arrest power on the premises they are assigned to protect, he said.

To carry a firearm, SPOs must complete a 40-hour training session and go through an eight-hour recertification program every year to stay active, Shelton said. About 5,000 SPOs are licensed to work in the District.

According to a Bureau of Labor Statistics fact sheet issued in June 2009 there were 84 fatal occupational injuries for security guards in 2007 up from an average of 68 per year from 2003 to 2006. Homicides made up the largest portion of those deaths at 51%, with a breakdown as follows: 47 % were committed by customers or clients, 33 % by a robber, and the remainder by an unknown assailant. In addition 13% of all injuries to security guards requiring a day or more away from work were related to

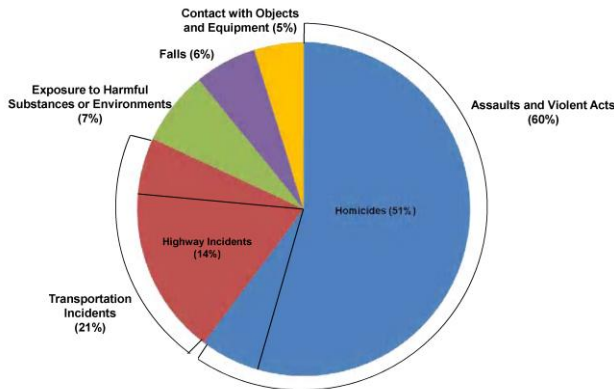
Security Guard Fatalities, 2003-2007



assaults and violent acts in the workplace.

The protection of people is a bond with a community, whether it's a city, a neighborhood or a confined geographical location like a museum or business facility. Mourning those who serve is an appropriate tribute whatever the source of their paycheck. Recognition of their service allows us to focus on the values we require to remain above the fray and loyal to our professional standards.

Fatalities to Security Guards, by Event, 2007



This incident is unfortunately reminiscent of the deaths of two U.S. Capitol Police Officers on July 24, 1998, who were shot at the entry way to the Capitol. Following their deaths Officer Jacob Chestnut and

Detective John Gibson were laid in honor in the rotunda of the U.S. Capitol.

For Officer Johns, the Holocaust Museum was closed in his honor and following his funeral his body was accompanied by the District of Columbia Metropolitan Police Department's Honor Guard to his place of rest.

We hope that from tragedy comes growth. Recognition of the dangers inherent in the security profession may require a higher degree of understanding by those who choose the profession, as well as those who train, manage and equip these important members of our society.

As Officer John's faced his God I hope he heard the words anonymously written for police officers as they meet their maker... "Step forward now, officer, you've borne your burdens well. Walk peacefully on heaven's streets; you've done your time in Hell."

THE FEDERAL BUREAU of INVESTIGATION REACHES OUT to COMMUNITIES ACROSS the NATION

Stacy Irving, Chairperson, Law Enforcement Transitional Training Committee, Law Enforcement Liaison Council, ASIS

Business, religious and community leaders across the United States have a unique opportunity to learn first-hand how the Federal Bureau of Investigation (FBI) works. As a participant in this extraordinary initiative called the *FBI's Citizens' Academy Program* which is currently being offered in all 56 FBI field offices, attendees are offered a chance to gain insights about the FBI as few others have. They hear about cases that focus on taking down organized crime rings or complex drug cartels, on fighting corruption to cases that involved civil rights violations, espionage and domestic and international terrorism.

Attendees hear real-life accounts from agents in the field about cases that required hundreds of hours and exhaustive field work, as well as behind the scenes glimpses of investigations that resulted in apprehensions that – in some instances -- required split-second, life and death decisions.

As has been said -- law enforcement is the only profession where you can *save a life, take a life or as has become painfully familiar in cities across the nation – lose your life.*

Attendees also have a privileged, behind the scenes look inside this unique law enforcement culture and special fraternity that has traditionally been closed to civilians since its inception. But all that changed in 1993 with a new perspective and the first Citizens' Academy Program.

And in 1996, Special Agent in Charge (SAC) of the Philadelphia field office, Bob Reutter, saw a critical need and the *Community Partnership Program* was born in Philadelphia. The program was modeled after the first FBI Citizens' Academy in Phoenix and was simply called "The Community Partnership Program" because that was -- and still is -- the primary goal of the program in Philadelphia and across the nation – to establish and maintain strong and mutually beneficial community partnerships.

The catalyst for the program in Philadelphia was a shooting of a fugitive by an FBI Agent from the Violent Crimes Fugitive Task Force in a quiet, working class neighborhood of Philadelphia.

Although the shooting was cleared -- or found to be a justified shooting – the community was in an uproar.

At the time of the incident scores of residents and community organizations were outraged and called for the agent's dismissal and an end "to this kind of FBI intervention". It was a watershed moment for the Philadelphia FBI.

The Philadelphia field office realized they didn't have established relationships with community leaders on whom they might rely as unbiased brokers to help them negotiate the delicate terrain of a suspicious and often aggrieved community. As a result, the Philadelphia Community Partnership Program (now referred to as the FBI Philadelphia Citizens' Academy Program) was created and I'm very pleased to report that in Philadelphia we have more than 400 local graduates to date and more than 10,000 graduates nationwide.

As FBI Citizen '*Ambassadors*' each graduate helps the bureau to better understand community perceptions or experiences, and helps to make lasting connections between the FBI and community and business leaders. This in turn helps provide a bridge to common understanding as to how federal cases are actually handled and how decisions are made, versus how federal law enforcement is often portrayed – and sometimes misunderstood – by the mainstream media. And following the tragic attack on September 11th, 2001, the program is even more important to the safety of our nation.

Sessions include learning the cool stuff; hearing about the tracking of spies and terrorists to forensics and technology, as well as the collection of evidence. Attendees get to spend a day at the firing range learning about guns and having a first-hand opportunity to handle and fire weapons. They even get to use the FATS machine to test their instincts and learn about the challenges of split-second decision making when choosing to fire or not fire one's weapon. They learn about tracking bank robbers to drug organizations to gangs. They sometimes get to hear personal accounts from former criminals currently in the witness protection program about life in the Mafia or other organized criminal groups. And just as important, attendees learn about the FBI's jurisdiction and congressional oversight. They also gain insights into the structure and operation of FBI field offices and resident agencies. Included in the class time is information about the FBI's policies, ethics and discipline, communications, civil rights, and future criminal trends.

Who attends? Business, civic, and religious leaders, each nominated by an FBI employee or a previous Academy graduate. Attendees must be at least 18 years old (with no prior felony convictions) and must live and work in the area covered by the field office sponsoring the academy.

Because classified techniques used in criminal and national security cases are discussed, nominees must undergo a background check and get an interim security clearance. Sessions are led by the Special Agents in Charge of that field office, their senior managers and special agent experts. Most Academy classes run 10 weeks-long with weeknight and a weekend session at the range. Many classes even get to travel to Quantico to see how FBI agents are trained and they participate in role playing scenarios at Hogan's Alley just like the *real* FBI Agents.

This is another great example of successful partnerships between the public and private sector. To find out more about Citizens' Academies, [contact your local field office.](#)

(Stacy Irving is a graduate of the FBI Philadelphia Citizens' Academy Program, currently serves as President of the FBI Philadelphia Citizens' Academy Alumni Association, is the former founding Vice President of the FBI National Citizens' Academy Alumni Association (FBINCAA) and is currently a member of the Board of Directors of the FBINCAA.)

From time to time things happen with computers that man cannot explain. Our June 2009 LELC Newsletter was an example of one of those times. Somewhere along the lines of passing the document from it's origin to publication it changed formatting. All of us strive for perfection, but we all fall short too. The Editor!

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

