ii. These five (5) California task forces were originally primarily funded through a State grant that requires a 25% match from local members.

iii. Has funding through State grant funds (which have been decreasing) and forfeiture funds

b. LAC Sheriff is the lead agency of SCHTTF.

c. Performs both high tech forensics and cyber investigations

2. Los Angeles Electronics Crimes Task Force (LAECTF[10]):

a. U.S. Secret Service is the lead agency.

b. Established by the Patriot Act, there were twenty-five (25) Electronics Crimes Task Forces (ECTFs) in 2008 across the country.

c. Performs both high tech forensics and cyber investigations

d. Has funding through US Congress and forfeiture funds

3. Orange County Regional Computer Forensics Laboratory (OCRCFL):

a. There are twelve (12) participating Agencies (including FBI-Los Angeles Field Office, most of the Orange County (OC) Police Departments, OC Sheriff, OC DA, California Department of Toxic Substance Control) and twenty-five (25) examiners.

i. FBI is the lead Agency with a Local Executive Board of member parties directing operations.

ii. Is the fifteenth (15th) such lab in the nation and one of the last two[11] "legacy" Regional Computer Forensics Laboratories (RCFL)

b. RCFLs do high tech forensics examinations only. The FBI's cyber investigation work is done by their Computer Emergency Readiness Team (CERT). CERT teams are housed at other FBI facilities.

c. RCFL provides approximately $13,000 in training during the first year, $9,800 during the second year and approximately $8,900 in subsequent years for continuing education and provides the equipment.

i. All forensic examiners must earn Computer Analysis and Response Team (CART) certification, which takes an average of fifteen (15) months.

ii. Every examiner/trainee receives individualized training based on their background.

d. RCFL offers IMAGESCAN methodology that they developed and provides free training on IMAGESCAN to law enforcement.

[10] With the passage of the USA PATRIOT Act, the U.S. Secret Service was authorized to establish a nationwide network of electronic crimes task forces.
[11] The sixteenth and final legacy RCFL is located in Albuquerque, NM

e. OCRCFL offers a cell phone kiosk (CPIK), a self service tool to facilitate obtaining digital evidence from cell phones. This is available to anyone in law enforcement.

f. OCRCFL has a system whereby they do the imaging, and the detective assigned to the case can come in and examine the digital data on a RCFL computer for evidence supporting his investigation.

4. Internet Crimes Against Children (ICAC) Task Force:

   a. This task force focuses on protecting children.

   b. Los Angeles Police Department (LAPD) is the lead agency.

   c. ICAC uses both high tech forensics and cyber investigations to thwart, apprehend and stop:

      i. Online predators of children

      ii. Child pornography

      iii. Human trafficking

      iv. Bullying

Other High Tech Crimes Task Forces and FLs

1. The LAC District Attorney's (DA) office has a High Tech Crime Division and FL:

   a. It conducts both high tech forensic examinations and cyber investigations.

   b. The DA is the lead agency.

   c. It is a member of both SCHTTF and ECTF

   d. Experts from this lab and office teach courses on cyber investigation and high tech forensics

   e. These courses are both POST and MCLE approved and taught worldwide

   f. A set of short training modules is being planned for Roll Call training

2. Municipal Police Departments in the County:

   a. Some do one or more of the following:

      i. Have in-house High Tech FLs

      ii. Participate in one or more of the regional task forces

      iii. Collaborate with neighboring Police Departments High Tech labs to create a local task force

   b. Others take all of the digital evidence they collect to SCHTTF or other regional task forces or to a neighboring Police Departments FL

   c. Some may not have embraced the inclusion of digital evidence in their crime fighting efforts either because:

i. Usable turnaround was not received when they tried

ii. Department has not realized its value.

METHODS AND PROCEDURES

This investigation involved tours of Task Forces and high tech forensic laboratories (FL), interviews with various law enforcement agencies, government entities, private companies and literature reviews. Several High Tech forensic labs were toured including: Arcadia Police Department (PD), Beverly Hills PD, City of Los Angeles PD, Culver City PD, Downey PD, FBI Regional Forensic Crime Lab in Orange County, Glendale PD, LAC District Attorney, LAC Sheriff, Monrovia PD, Redondo Beach PD, Santa Monica PD, Secret Service Electronics Crime Task Force, Torrance PD, Whittier PD.

The most recent District Attorney's annual law enforcement high tech crime survey, sent out in January 2011, included five (5) questions drafted by the CGJ regarding high tech FLs. This survey was sent to the forty-five (45) police departments in the County. The CGJ used the answers to the FL questions to determine which departments had a high tech forensics lab or used one of the regional labs in the County. The CGJ received responses from 91% of those surveyed. Of those responding, 38% had sworn personnel assigned to high tech forensic positions. Of the remaining 62%, most stated that they occasionally sent digital evidence to a neighboring or regional lab for analysis, which would typically take six (6) months to over one (1) year to receive results. This was often after the case had been completed.

FINDINGS

The high tech FLs and cyber security staff are part of a small cadre of highly motivated sworn and non-sworn men and women. All staff interviewed in the course of this Report are continuously improving and providing valuable services to support the safety of LAC and its cities and communities. However, their efforts are hampered by insufficient funding for training, staffing and resources.

FL Models

There is not a one-size-fits-all answer to the FL needs for the greater Los Angeles area at this time. Several successful FL models are moving forward in different parts of the County. What is clear is that additional FL resources are necessary, as well as more trained sworn personnel, more training, more hardware and software. Further, continuous improvement is a necessary part of this high tech arena. Ongoing training, hardware and software updating, software licensing, best practices development and redevelopment in the face of the ever changing technology and tactics being deployed by the crooks, nation-states, and cyber terrorists is required.

During tours, the CGJ observed that four (4) approaches or models of FLs currently operate in LAC. These models, briefly described below, provide alternative ways to tackle incorporating high tech forensics into local police work and bringing FE and CI to bear for the safety of the public.

1. Regional Joint Task Force Model:
    a. RCFL, ECTF, SCHTTP and ICAC are each excellent examples.
    b. Provide for easy collaboration, flexibility of staff allocation, leveraging of multi-agency funding and resources and mentoring
    c. Membership may be formalized through a Memorandum of Understanding (MOU) or an informal agreement.
    d. Improved service on a regional scale
    e. Maximize Federal, State and County resources

2. Localized Joint Task Force Model:
    a. A well structured example of this model included:
        i. Three (3) neighboring cities with the FL located in the Police Department of one (1) of the cities
        ii. Four (4) sworn officers from the three (3) cities
        iii. Two (2) sworn officers from two (2) RTFs
    b. Membership may be formalized through an MOU or may be informal.
    c. Supported by the citing city's Information Technology (IT) Department
    d. This FL is a member of SCHTTF and TF
    e. Provides for easy collaboration, flexibility of staff allocation, leveraging of multi agency funding and resources and mentoring
    f. Improved service to participating cities constituents

3. Loosely aligned group of single jurisdiction FL:
    a. The FLs are located in the Police Department of each of the cities.
    b. The FL is a one-officer or one- tech shop.
    c. Association is loosely structured and based on a mutual aid model.

4. Single jurisdiction FL with membership in Regional Joint Task Force(s).
    a. The FL is located in the Police Department of that city.
    b. The FL has one (1) to five (5) trained staff, generally a combination of sworn and tech.
    c. Is available to other law enforcement agencies on a mutual aid model

FL Skills and Equipment Considerations

1. A well equipped high tech forensics lab should include these skills:
    a. Collecting and seizing digital evidence
    b. Duplication, storage and preservation of digital evidence
    c. Impartial examination of digital evidence
    d. Personnel trained in high tech forensics and/or cyber investigation
    e. Investigators trained in courtroom testimony
2. FL equipment and layout:
    a. It is beyond the scope of this Report to recommend equipment. However, existing labs within LAC and OC are excellent resources for this type of information.
    b. Equipment requirements fall into several broad categories, including hardware, software, storage, software licensing, cabling, fiber optic networks, firewalls, encryption, etc.:
        i. Should be housed in a secured area
        ii. Workstation area can be common or individual
        iii. Should include a server closet and/or removable hard drive storage
        iv. Evidence intake area
        v. Evidence storage area
        vi. Some area that allows for a static free work space

Risk Management Approach

The high tech forensic arena, like a mine field, is rife with risk. Whether dealing with cyber security, cyber investigation or forensic examination, applying the tenets of risk management to the discipline and effort will facilitate achieving best results and best practices.

The basic rules of risk management are Recognize, Prioritize, Mobilize (RPM)[12] The list below includes some of the components that support RPM implementation for high tech forensics:

1. Continuous Improvement
2. Crafting the vision and political will to prioritize and reallocate budgets to address crime fighting needs in the digital age
3. Have a sufficient number of equipped and trained FE and CI to do the job in a timely manner
4. High quality training
5. Highly motivated staff
6. Highly qualified staff
7. Improved service to constituents as a goal

[12] Graham, ibid.

8. Procurement guidelines that recognize and take into account the rapidity with which technology is changing
9. Systems to monitor best practices, compliance and changing technology and to reward performance

Training

In employing the RPM approach in any field, including high tech forensics, training is a core ingredient. The purpose of training must be to create officers who are prepared, equipped, and ready to perform and respond to any situation that presents itself. Anyone can train personnel after something goes bad[13]. The real challenge is delivering training proactively to prevent problems prior to occurrence.

If trained personnel are not available to utilize a FL, then it is largely an expensive box with equipment and software that is lying fallow and becoming obsolete. Whether it is a State of the art new regional FL or a small FL in a converted area of an existing facility, it requires well qualified and well trained personnel.

High tech is a fast evolving field; continuous improvement is the name of the game. Today's new "thing" may be out of date tomorrow. Today, most hard drives are magnetic, but the trend is towards switching ceramic hard drives. Storage is moving to the "cloud." And so on. The cyber intruders, terrorists and crooks are continuously improving their mode of attack, trying and developing new tactics, software and hardware. Our forensic examiners and cyber investigators have to be continuously improving as well. Training is critical and MUST be ongoing as the technology is always evolving.

1. The CGJ heard from several sources that it takes about three (3) years to bring someone new up to speed, one (1) year of training, one (1) year of mentoring and one (1) year of seasoning. Somewhere between mentoring and seasoning, more training is probably needed due to technology developments.
2. There are insufficient funds to train existing detectives.
3. There are not enough trained forensic detectives to process all the digital evidence in a timely manner.
4. Some excellent training is available in the Cyber Security, cyber investigations, and high tech examiner arenas by both government and the private sector. Some of the government agencies offering high tech training classes include: US DOJ, DHS, SS, and California DOJ. The DOJ training attendance is awarded through a nationwide lottery. The training is excellent.
5. Training in the seizure, handling and analysis of digital evidence, should be made a part of the Commission on Peace Officer Standards and Training (POST) training programs for sworn personnel. This allows the use of the available training dollars to support the high tech aspect of sheriff, police and detective training and expertise.
6. Only some of FE and CI training, as of the writing of this Report, is part of POST training programs for sworn personnel. This places limits on the training dollars that are available to support this aspect of sheriff, police and detective training and expertise.

[13] Graham, ibid

7. High tech forensic training is not currently part of basic training for police or sheriff recruits in LAC, and may or may not be included in detective training. It is not required training for DAs or judges either. It should be.

Promotion, and Succession Planning

1. To promote in law enforcement departments currently, you have to leave high tech forensics/cyber investigations and return to patrol. Those trained and skilled in high tech must leave the discipline, resulting in a loss of the continued benefit of their expertise and skills, which lie dormant and atrophy when they return to patrol in order to move up in the organization. In addition, the department must incur the costs of training someone new to fill the then-vacated high tech position.
2. Succession planning is highly valuable in the high tech arena so that the new examiner/investigator gains knowledge through receiving mentoring from the sitting expert(s) before they move on.

Digital Evidence and Procedures to Address Detected Intrusions

1. Digital evidence is critical in solving "high tech" crimes:
    a. Digital evidence is always available in high tech crimes and almost always available in "old school" crimes[14], and may be critical to reaching a successful conclusion to a case.
    b. While difficult to quantify, it is possible that digital evidence, by closing a case and getting a criminal off the street, may be cost effective simply by preventing a criminal from re-offending, getting arrested again and processed repeatedly before finally being convicted.
2. Procedures to address detected intrusions into government[15] infrastructure computers are in place; however, better policies and procedures for a coordinated response and updating of procedures are needed:
    a. Protocols for notification of internal breaches are formalized in both the County and the City.
    b. The City of Los Angeles has a formalized protocol for calling in the best available resources to respond to a threat.
    c. In LAC, there may be a need for periodic reassessment of the best internal resources to bring to bear for responding to and investigating high level threats.
    d. In areas where critical infrastructure is provided by private industry/third parties, LAC either has no formalized notification, response protocols or MOU in place, or it was classified in a way to which the CGJ was not made privy.
    e. A formalized protocol is critical to a timely effective response.
        i. It is important from a succession planning standpoint to document the institutional knowledge because, while the current personnel may know whom to call and what resources are available, a change in personnel risks allowing such informal knowledge to slip through

[14] Murder, arson, rape, kidnapping, burglary, robbery, battery, assault, etc.
[15] Los Angeles County and the City of Los Angeles (no other cities were queried on this subject):

the cracks. Communications at a critical juncture might then fail or be too slow.

ii. Policies and procedures must be developed and reviewed so that they support a continuously improving ability to detect intrusions and protect critical infrastructure and data.

RECOMMENDATIONS

1. The District Attorney, being the nexus of all law enforcement in the County as prosecutor of felonies, should take the lead role and become the central repository for coordination of high tech information by doing the following:
    a. Establish and keep up to date a list of all training available for high tech forensics examination, cyber investigation and cyber security, including local, State and Federally sponsored training, as well as private training opportunities. It is likely the DA's high tech Forensic Division is already doing this internally and could, with little effort and cost, make this information available to the Task Forces, the LAC Sheriff and the municipal police departments.
    b. Provide outreach to all police departments and the sheriff on a regular basis regarding the value of and training in high tech forensics in crime fighting in Los Angeles County.
        i. This could be done through seminars for groups of law enforcement officers organized geographically by Supervisorial District or area; e.g., South Bay, San Gabriel Valley, West LA, San Fernando Valley, etc.
        ii. Individual department "roll-call" training should also be part of this program.
    c. Keep a log of the use of digital evidence in the prosecution of cases, both high tech crimes and "old school" crimes. The log should indicate the nature of the digital evidence (cell phone photo, location info, contact info, computer file, GPS, etc.); its importance to the case (useful, important, critical); and the role it played (allowed case to settle, critical to achieving a guilty verdict, sentence enhancements, freed an innocent person, enabled the return of stolen property to rightful owner, etc.). The DA should encourage municipal departments to do this for misdemeanors as well. This will build a body of evidence to help inform decision makers in the budgeting process and persuade law enforcement agencies with no in-house capability to see a need.
    d. Establish a program for all deputy DAs to acquire the basic knowledge and skills necessary to develop their cases using digital evidence in a manner a judge and jury can understand
    e. Develop and conduct seminars to educate the judges in digital evidence use in the criminal justice process

2. Arcadia PD, Beverly Hills PD, City of Los Angeles PD, Culver City PD, Downey PD, Glendale PD, LAC District Attorney, LAC Sheriff, Santa Monica PD, Monrovia PD, Redondo Beach PD, Torrance PD, Whittier PD.

a. Establish a “High Tech Forensics Bureau.” This will facilitate:

    i. Promotions and career opportunities for those who are trained and skilled in this area without having to leave the discipline

    ii. Succession planning and transfer of high tech expertise, preserving the investment made in creating the expertise.

b. Update regular law enforcement recruit and detective training to include orientation, procedures, protocols and other training with respect to digital evidence

c. Include training in digital evidence collection, analysis and use in “roll call” training.

d. Take steps to acquire the POST certification for High Tech training courses for forensic examiners and cyber investigators to allow for reimbursement of the costs.

3. LAC Chief Information Office and Internal Services Department should conduct internal reviews concerning cyber security and infrastructure protection from Cyber attacks and terrorism:

    a. LAC must have protocols, policies and procedures facilitating timely, efficient rapid response by the most able cyber security resources available and ancillary emergency response by other agencies, if warranted, in the event of a cyber intrusion, fire wall breach or other cyber attack.

    b. These should include coordination with key third party vendors. Many basic services within the LAC are provided by third party vendors. The Metropolitan Water District and California Edison are two (2) examples.

4. The LAC Board of Supervisors should task their lobbyist in Sacramento and Washington with looking at opportunities to redirect fees and taxes on land line phones, cell phones or internet access services to provide funding allocated to the support high tech forensics, cyber security and forensic examination programs

5. LAC and the City of Los Angeles establish a "High Tech Endowed Badge Program” to support the training and equipping of FE and CI throughout local law enforcement. Initially, establishment of eight (8) EBs could be evaluated. Setting up five (5) EBs by the LAC Board of Supervisors District one for each Supervisorial District; and setting up three (3) EBs by the City of Los Angeles one for each of the Proprietary Departments (Department Of Water and Power, the Port of Los Angeles, Los Angeles International Airport (LAWA)) for a total of eight (8) EBs.

Funding Training through an Endowed Badge – A Concept

Borrowing a concept from the University system, the CGJ believes there is a future in establishing, within law enforcement, a High Tech Forensics Examination – Cyber Investigations – Cyber Security Endowed Badges Program. If possible, these could be “named” endowed badges (EB). It is in the interest of business to have a safe City/County in which to do business. There may be interest from many sectors to participate in this EB public private partnership.