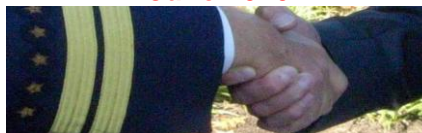




LAW ENFORCEMENT LIAISON COUNCIL

June 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.

Interpol Committee
Mr. Carlos Velez

Membership Committee
Mr. James W. Birch

Publications Committee
Mr. Robert E. Lee, Jr.

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,

This month I will follow-up on cyber-vetting activity. The IACP-PERSEREC focus group sessions on cyber vetting are proceeding, with an objective of wrapping up by early August. Draft guidelines for Internet vetting and cyber posting are being modified by peer review from all types of participants, including ASIS members. LELC members are participating and hosting some focus groups. Among the interesting developments to date is that several law enforcement agencies are requiring police officer applicants to sit down with background investigators and log onto the social networking and other websites frequented, to show that their postings are proper. Refusal to do so results in no police job opportunity. Police have also found that defense attorneys are trying to use officers' Internet postings to impeach their testimony on the stand. In one New York case, a defendant facing gun possession and resisting arrest charges claimed he was set up, and his attorney brought out the arresting officer's postings showing his "Training Day" mentality. The defendant was acquitted on the gun charges, and convicted on the lesser resisting count. -Ed Appel

Protection through Written Policies

Submitted by: James D. Brown, LELC Member

Written policies and procedures are a major tenant of management organization and provide direction to employees in carrying out their duties in an efficient and effective manner. This is particularly true of the security function of a corporation because at some time, something will go wrong. Among other things, a review of the guiding instructions generally results from the aftermath of a serious negative situation. If the written guidelines were appropriate, the issue then goes to training. Were employees properly trained and had periodic training updates? Was re-qualification required and was it completed? Was the training documented? Was the instructor qualified? Were there written lesson plans that were reviewed and updated as necessary?

After training, supervision becomes the issue. Can the organization document that they provided adequate supervision and taken action in the past to correct problems? Nearly all these issues can be documented to a significant extent with various business records or files. Doing these critical basic steps can protect the organization, limit loss

and liability exposure, and may also provide a manager with deserved protection after a negative incident.

Because written directives are one of the bases of our management strategy, some guidance on writing policies and directives will be helpful. Many terms are used interchangeably and often technically incorrectly. This *technically incorrect* can sound venial but it can be a major factor when responsibilities are being determined, whether it is by the organization, the media, or the courts. The following are common terms that need to be understood when writing policies, directives, or instructions.

- *Organization values* are the beliefs of the organization, its ethics and conduct.
- *Goals* are broad statements of what the organization wants to accomplish or attain.
- A *mission statement* is more specific and generally relates to how these goals are obtained.
- A *plan* is a method of accomplishing something or responding to a situation in the future.
- *Policies* are broad statements of principals that provide a framework for directives, procedures, and rules.
- *Rules* are generally clear instructions on what to do or not do in certain situations and are not to be broken.
- *Directives* are specific written instructions or information that is generally topical.
- *Procedures* are step-by-step actions to consider or take depending on the specific situation.
- A *memo* is a method of communication information on a specific issue and is often temporary guidance (if the guidance is permanent change the directive). This is basically the same as *special instructions*.
- *Reviews* are supervisory checks of employee actions or work product to ensure they meet organizational standards.
- An *analysis* is a critical review of all the relevant available information, with logical conclusions deduced from the compilation.

Additionally, once policies and procedures have been drafted have them reviewed by knowledgeable people, including those that are expected to comply with them. This enables improvements or corrections to be made promptly and efficiently. More importantly it also increases the buy-in of effected employees.

Traditionally the most difficult part of achieving compliance with policies is the reluctance of first line supervisors to implement and maintain policy compliance. It is sometimes easier for the first line supervisors, male or female, to be one of the “guys” and infer the organization’s policies are from inept management. Once an incident occurs the same people may point to general ignorance of policies as the corporate norm or point out other exceptions to avoid responsibility. Obviously, this makes management’s problem more difficult.

Problems may be abated through a sound written directive system.

[A Win-Win Deal](#)

By: Carlos Velez, Member, LELC

Back in 2003, during the winter time, I was told to represent Johnson & Johnson in a three-day planning meeting to be held in Buenos Aires Argentina, under the auspices of Interpol (www.interpol.org). I was instructed “to fully cooperate with the sponsor entity in any security matter to protect the company’s interests”. With that clear mission and knowing nothing about the specifics of the meeting or who the participants were, I arrived the first day to the meeting room and began as usual, exchanging business cards and meeting people including the Interpol representative at that time, Mr. John Newton, a British national who graciously welcomed the participants. After five minutes of his introduction, I realized that Interpol under the leadership of Mr. Ronald Noble, was putting together a vast number of resources deployed from Lyon, France and also from their regional offices, to the service of the private sector representatives as a vehicle to tackle common problems: Intellectual Property protection related to international crimes.

The planning meeting resulted in what is today known as Operation Jupiter, that involves law enforcement agencies from several countries in South America, and representatives from several industry segments such as music, video, apparel, pharmaceuticals and tobacco.

Six years after that cold winter meeting, the results are on the table: Interpol has been the facilitator between the private sector and the law enforcement agencies in the countries to conduct raids, to confiscate fake products and to produce more intelligence to continue targeting the sources of the problem.

In tangible numbers there have been five Operations Jupiter over the past six years, millions of dollars have been confiscated in products, hundreds of people have been detained and prosecuted and dozens of sources have been targeted. Thousand of police officers, custom officers, attorneys and other public officers have been trained by the private sector. More importantly, consumers can be assured of high quality and safety of purchased products because the can be reassured of the conditions in which the products have been manufactured, transported and stored.

Mr. Noble and Newton are the authors of this initiative. There is a tremendous gratitude toward to them because they both understood the problem and identified a key region to target. And more important, both were able to articulate, like in a concert symphony, sometimes two discordant entities: The private and public sector. And in the song "Operation Jupiter" one plays the melody and the other one plays the rhythm.

Welcome ASIS to this win-win deal.

The Art and Science of Risk Assessment

Ira S. Somerson, BCFE, CPP, CSC, Member LELC

Failing to preface your security plan with a risk assessment would violate standard security industry practices. If your risk assessment lacks sufficient qualitative (unscientific) or quantitative (scientific) analysis, your security program will probably be below a standard security industry practice.

Mary Oscalli was attending an up-hill dirt bike race in a popular mountain resort. The event had been held each summer for years and was always scheduled over the Fourth of July weekend. The land was leased to a promoter who used the winter-time ski area for uphill bike racing enthusiasts. Bikers from all over the state gathered for this event. Food and beer were served as local musicians entertained the fans. Attendees, between races, would lay out on the lawn and picnic. As the day wore on and beer continued to be consumed, it became a dominant factor in the festive mood of the crowd. Besides the festive atmosphere, some grew irritable and a few disagreements flared up. Security officers assigned to the event were quick to isolate and contain these problems. Off-duty police officers were also deployed. Throughout the event attendees could hear firecrackers going off. On occasion, loud explosions were heard. The concussion from these devices could be felt some distance away. Those detonating the devices usually moved away from the crowd when they lit the fuse and tossed it in a safe direction. They were "cherry bombs." Some were larger devices. Everyone knew this; so did police and security. It was part of the event and its past. This was a "bikers" crowd. What's the problem! Neither the promoter, the police nor its security officer service had anything to do with sanctioning or providing the fireworks. Neither did the promoter, police or security do anything to ensure that the fireworks tradition was conducted in a safe manner. Some teenagers, who were able to purchase and/or consume beer and who were tossing the cherry bombs decided to have some fun and tossed one in the direction of a crowd of other teenagers nearby. The device deflected off a tree and landed directly alongside Mary Oscalli and her pre-teen children sitting on a blanket having lunch. When she saw this device land within inches of one of her children, she instinctively reached for the device to throw it out of harms way. The device detonated in her hand. Mary lost three fingers. Her son suffered a hearing loss.¹

Consider these questions:

- Was this event foreseeable?
- If the event was foreseeable and the event's promoters or security services knew or should have known that an accident with fireworks could occur, what should their security program have been?

Risk Assessment is the art and science of identifying security vulnerabilities, measuring the ***likelihood*** that each vulnerability will occur (foreseeability), the ***opportunity*** for each to occur, measuring each event's ***impact*** upon the organization's assets (criticality) and ***prioritizing*** each identified vulnerability in comparison to all others (queuing).

¹Theresa and Joseph Keene v. White Rose Motorcycle Club, Inc. et al, Jefferson J. Shipman, Esq., Goldberg, Katzman & Shipman, P.C., Harrisburg, PA, 1996.

Partial Range of Other Definitions

- Legal: The legal definition of Risk is “...the element of uncertainty in an undertaking.”
- Financial: “...the ultimate cost to an organization for failing to identify vulnerabilities and develop deterrent/remedial programs.”

Standard Security Practice

The variety and causes of security risks are considerable. For that reason, some formal process must precede any security program implementation. A security program’s design needs to have the objective of deterring, detecting, delaying, denying, responding to, and/or recovering from reasonably foreseeable events. The fact that anomalous events do occur should not excuse or rationalize an organization from not first performing adequate planning. It is inevitable that a property owner will fail to recognize every risk or that an event will occur in spite of adequate planning. But the fact that an adequate process was not used to identify the levels of risk places an organization in a far more egregious posture. Failing to preface your security plan with a risk assessment would violate standard security industry practices (standard of care). If your risk assessment lacks sufficient qualitative (unscientific) or quantitative (scientific) analysis, the program will be below a standard security industry practice.

*“Risk analysis is central to the security countermeasure selection process. It is used as the basis for design engineers and security managers to select from a wide range of available physical, electronic, operational and procedural countermeasures... The end result is a security design concept upon which subsequent phases of design can be based. But even after the final design is completed and the system is installed and operational, risks must be regularly evaluated according to changes in assigned assets, perceived threats, and opportunity for asset compromise based upon new exposures or outdated countermeasures.”*²

*“Risk management is a disciplined approach through which uncertain events can be identified, measured, and controlled to minimize loss and optimize the security returns on the investment dollar...”*³

The mission of security management (e.g. loss prevention, asset protection, etc.) will be below a standard security industry practice if it fails to:

- Identify reasonably foreseeable risks.
- Tests and continues to monitor the existing security program in response to the foreseeable levels of risk

What Should a Risk Assessment Consider?

In conducting risks assessments, the process should include:

- Operational aspects of a facility and its “inherent” risks.
- Perceptions of the facility or operation by the public.
- Perceptions of the facility or operation by its employees and contractors.
- Public statements and lifestyles of high-profile executives and employees.
- Demographics (“social disorder”) of the community where the facility is located.
- Demographics of the facility’s work force.
- Nature of neighboring properties.
- Access roads to facility.
- Police and/or a facility’s incident history and the history of security events occurring at the subject location.
- Facility management of its property and resources.

2. Risk Byline, Michael J. Stedman, Security Technology & Design Magazine, May, 1999.

3. Risk Analysis for the Security Manager, Datapro Research Corporation, based on EDP Security Risk Analysis: A Technique for the Security Manager,” by Nander Brown, October, 1966

- Efficiency of a facility's existing security strategy.

Examples of "Qualitative" Risk Assessment:

- Facility's perimeter and community surveys.
- Police Department and other community interviews.
- Employee and contractor interviews.
- Process and operational surveillance and studies.
- Analysis of existing physical and procedural security.

Examples of "Quantitative" Risk Assessment:

- Benchmarking all facility's operated by the organization to determine risk levels and a standard of care.
- Benchmarking competitive or similar facilities to identify a standard of care.
- Analysis of public police (dispatch and/or incident data)
- Analysis of an organizations in-house incident data.
- Reference to and use of strategy (security practices) evolving from scientific research.

Discovery and Investigation of an Organization's Security Program:

Discovery and investigation of premises security matters should seek to identify:

- Did the organization routinely conduct qualitative and quantitative risk assessments?
- Was the assessment performed using a qualified methodology?
- Has the organization determined the operational aspects of a facility and its "inherent" risks?
- Were qualified persons used in conducting the risk assessment?
- Can the organization illustrate changes in their security strategies in response to a continuing risk assessment program.
- Has the organization sought in-house or outsourced expert support?
- Has the organization ignored the advice of existing security vendors or inside requests for support?
- Demographics ("social disorder") of community and/or organization.
- Nature of neighboring properties.
- Access roads to facility.
- Police and/or a facility's incident history.
- Facility's management of its property and resources?
- Efficiency of a facility's existing security strategy In evaluating certain incidents it would also be helpful to determine:
- Has the organization sought to identify the perceptions of the facility or operation by the public.
- Has the organization sought to identify the perceptions of the facility or operation by its employees and contractors?
- Has the organization sought to identify public statements and lifestyles of high profile executives and employees?

"Risk analysis remains the cornerstone of any security program, and it is the fastest way to gain a complete understanding of your organization's security profile - its strengths and weaknesses, its vulnerabilities and exposures."⁴

Inherent Risks:

When you ask someone what is the primary risk in a convenience store operation, the usual answer is "robbery." Others may say shoplifting, but from the point of view of criticality and the potential for

4. A White Paper on a Value-Added Model for Security Management, Stephen Gale, Keith Duncan, Rudolph Yaksick, John Tofflemire, Research Supported by the American Society for Industrial Security Foundation (ASIS), December, 1990.

violence and/or loss of intrinsic assets, robbery would be the likely choice. Some will argue that not **all** convenience stores are equally vulnerable to robbery. This is true. But the fact remains that its basic operation (without adequate deterrents) makes it uniquely vulnerable to this particular crime.

Although a bar and night club may also be vulnerable to a robbery, the same response in this environment would probably be “aggravated or simple assault” (fighting). A department store? Shoplifting. A parking lot? That would depend upon where the parking lot was, but usually theft of or from auto. A high-rise residential building? burglary and/or various assaults. These examples are generalizations that require far more study, but explain why evaluating inherent risks in a business operation is strategic in developing a security program. A security program should never be developed **solely** on the basis of anecdotal or experiential instincts. But they **should be** included in the risk assessment paradigm.

It’s too easy to draw conclusions from instinct or professional and business experience. What are some of the other resources we can use to identify **inherent risks**?

- Research: Most organizations are linked to a business, trade or professional association. More often than not, these organizations have studied and/or published materials that identify unique risks.
- Legal Research: Most industries and/or organizations have been the target of civil litigation. Database research with highly regarded search services can provide a wealth of data concerning an organization’s vulnerabilities.
- Underwriter Data: Many organizations who have recognized their security risks have chosen to insure against its potential and purchased insurance rather than spread the risk or self-insure themselves. A risk management and/or underwriter’s loss control department can be an excellent resource to identifying risk.

Why are organizations vulnerable to criticism of their security programs?

Organizations are reluctant to document their failures and view security breaches and potential risks accordingly. Efficient and economical software already exists to track and generate useful security incident data. The trick is to create a policy and procedure with management’s strong support that ensures employees **will report** incidents the very first time they experience an incident or reasonable suspicion. Instead, senior management and house counsel persistently avoid doing this pointing to their concern of it creating a self-incriminating record. In fact, failure to understand one’s history and risks is the best route to self-incrimination. If employees believe that their customers and their own best interests are served, they **will** support a well developed incident reporting and loss tracking program. Discovery and investigation will more often than not identify that organizations do **not** perform this vital function and are therefore doomed to persistent security incidents.

Unfortunately security managers are **not** taught security management in business schools. Most security problems are business and people problems, but still no serious effort exists (with an established business school) to provide this important curricula to future business executives.

Security is taught within criminology curricula, but that is more like preaching to the choir. As a result, a business organization’s operation is usually not structured to **include** and coordinate security oversight. It is often left to others, not qualified to understand security risks, to assume this important stewardship. This could be an argument for hiring a security manager if your organization does have unique and developed security threats, but it also begs the issue of ensuring that other disciplines within an organization **include** analysis of security threats in their agenda. For example: audit, safety/environmental, operations, human resources, legal and/or facilities are routinely exposed to security issues.

Senior management of most organizations believe that a security function is purely a cost center and does not produce any “net present value” to their organization. For this reason, discovery and investigation will very likely reveal that security departments and/or functions are routinely downsized or eliminated exposing their organization to serious threats. Their objective is economy, but the very

opposite will often occur. *“The responsibilities of security directors are evolving from “locks, bolts, and badges” (Felson, 1988) and perimeter protection to a more sophisticated involvement in organizational management. Confronted with novel, complex security exposures and attendant risks, traditional security functions are becoming only a part of the larger overall responsibilities of security directors. Given this evolution, the motivating problem of this paper is: What is the best approach to managing the growing complexity of corporate security threats so as to provide minimal security losses, for a particular level of investment in security? This paper argues that to provide an optimum level of security service to the organization not only must the security department be repositioned within the modern corporate but that its management required the development of a new paradigm of organizing security functions. The approach taken here to developing such a paradigm focuses on demonstrating the weaknesses of a cost center management approach, which is considered representative of existing security management practices, and on advocating the strengths of moving toward a profit center management approach...”* instinctively, persons who do not normally design or implement security programs think of strategies (e.g. electronics, security officer services, etc.) *before* they consider risks. I was once interviewed for a consulting assignment with a large manufacturing organization that asked me what type of security program I thought was required. I answered the question with a question. “What type of risks are you trying to prevent?” I explained what has been outlined above. From the onset my potential client was “thinking” and “visualizing” a security system that kept “bad people out,” but didn’t understand what was at risk and why they objectively needed a security program. After approval was granted for a thorough risk assessment, it turned out that the client’s intellectual property was significantly at risk and, in fact, was being victimized. Other issues were also developed, but the shape of the security program took a significantly different turn once they understood their true vulnerabilities.

Reasons for Failure

Why do organizations persist in having incidents of violent crime? Why are their employees and business invitees exposed to serious security risks? Organizations usually look for quick fixes to problems that they believe are within their area of stewardship. Having never had any serious exposure to the art and science of security management, they are likely to feel that they have the ability to conserve and protect their assets (people, information, property and reputation) without expert support. Unfortunately, “security” is usually folded in with the image of the “rent-a-cop” at the entrance or “those things that you put on doors,” etc. It’s easier to keep it simple than to admit you are vulnerable or unaware of how to manage a serious problem. It may also require capital investment and/or operational outlays (this will serve as an excellent rationalization for doing nothing). As with most management problems, security is a complicated process requiring knowledge of a significant body of knowledge. Security risks do not disappear simply by buying “things” and wish it will then go away. As with all business problems, it requires data to arrive at a strategic plan. Victims of crime are more often victimized by:

- Lack of strategic interest in security by senior managers, property managers, etc.
- Lack of understanding of security issues;
- Lack of adequate study of security risks;
- Lack of commitment and investment to security strategies;
- Deflecting the responsibility for security to others (e.g. law enforcement, other unqualified staff functions, etc.)
- Failing to understand the “net present value” of security management services.

Risk assessments are not a panacea, but failure to use this process in forming a security program should be mandatory and in most cases failing to do so will lead to a poorly planned security program.

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

