CHAPTER 2

SECURITY VULNERABILITY

Overview of Chapter 2

Part I of this Chapter states that no security program can be effective unless it is based on a clear understanding of the actual risks it is designed to control; and that the value of a program depends on its appropriateness and the relevance of resources. Measuring devices are then described, and both a vulnerability survey form and an outline for a basic matrix are provided. cost effective security planning is explained and emphasized.

Part II discusses a team approach (security professional and functional managers) and provides a guide to examining the concept and assessing its usefulness. Practical steps to initiation of a program are included, as well as follow-ups and audit control.

Part III discusses security from the budgetary point of view and examines the role of the supervisor in loss prevention for companies that do not have a security department or professional. Theft scenarios are given and an ‘‘events breakdown’’ analysis method applied; a rational sequence to security requirements is explained; and a recommendation to develop positive security contracts is outlined.

CHAPTER 2
Part III

ENGAGING EMPLOYEES TO PREVENT LOSSES

The security program in many organizations generally consists of access control and after-the-fact investigations. While these activities are important facets of an assets protection program they fail to address the real source of much of the loss problem. The objective of an assets protection program is the prevention of loss; however, the program often does not take into consideration regular minor loss events within the individual work units of the organization. Examples include the misuse of equipment and facilities, careless handling of raw materials and finished goods, sloppy documentation and poor inventory controls. These events that occur during a normal work-day routine can lead to major losses if not corrected or modified.

A widespread attitude in many enterprises is that asset protection measures are the exclusive task of the security organization. Most enterprises—almost all large ones which have formal security programs—devote at least some time to security orientation or security awareness. However, knowing that a security program exists is not the same as playing an active role in loss prevention. There are specific activities that non-security personnel can and should incorporate into their own everyday routines that will enhance the entire loss prevention effort. Every department and function has a necessary role to play in the identification, prevention and reduction of losses.

Among the many methods for including the entire work force in the loss prevention effort are two techniques by which security investigations and vulnerability assessments can be integrated throughout the organization. The first technique applies *multilinear event sequencing* to the investigative process. The second technique involves the application of the *critical incident review*[1] as a device to predict additional vulnerabilities that might otherwise remain undetected until after a loss had occurred. Both techniques involve supervisors at all levels as catalysts to promote security thinking by the workforce.

MULTILINEAR EVENT SEQUENCING TECHNIQUE

A review of the basic investigation process is helpful before engaging in a discussion of the multilinear event sequencing technique in detail. In every investigation the investigator is confronted with the need to answer the question: *What really happened*? The usual process is to reconstruct the prevailing conditions at the time of the incident and to isolate those events suggested by the evidence obtained at the scene of the loss. As the investigator learns more about the events that occurred before the loss, a rough picture of what happened begins to emerge. As additional evidence is developed, the investigator begins to speculate about how the theft or other loss may have occurred. Each possible scenario is tested against the evidence to arrive at the most likely explanation.

This investigative method is based upon the assumption that someone does something that results in a loss of property. Each event influences, or is influenced by, one or more events that either preceded or followed it in time. It is the precede/follow logic of the related events, and the simultaneous visual display of them in the form of a probable scenario, which lead to the inductive methods so prized by investigators.

The investigator is applying inductive reasoning using an *event breakdown* method. The gross event—perhaps a theft—is broken down into related events which preceded or followed it as the questions of *who, what, why, when, where* and *how* are answered. Each time an event is subdivided, the need for a more precise understanding of the actor-action relationship arises, and the whole questioning process is repeated. The last known action provides a starting point to hypothesize the next action or actions which probably occurred, as supported by the evidence. The connecting of events is suggested by logical, spatial and temporal relationships among them as they progress through the precede/follow sequence.

This method of breaking down the sequence of events leads to the discovery of unknown events required for the sequence to have proceeded from beginning to end. For someone to

[1] These terms were applied to security loss analysis by the late Robert D. Donovan, CPP, who originally developed this chapter.

do something which leads to a loss, certain enabling conditions must exist. The creation of these conditions also flows from an event sequence, which, in turn, produces changes of state or outcomes. For any matter under investigation, a description of the chronological flow of events can often provide an explanation of what actually happened. This is similar to the way in which we create visual images when we try to describe an event or listen to descriptions provided by others. The existence of the enabling conditions can be traced back in time to explain the why and how of the loss event sequence. This will either lead to a solution, or to an inconclusive termination because of the lack of hard evidence upon which to construct an event sequence.

A major complicating factor in many investigations is the complex nature of most business organizations that seldom affords the investigator a clear-cut view of a theft case. The initial fact to be established is that a loss has occurred (i.e., company assets have left company control in an unauthorized manner). Overlapping areas of responsibility and joint use of facilities often leave the investigator with multiple participants in the possible loss process. In these cases, the investigative method involves setting out the actions and behavior for each participant in the sequence needed to produce the loss. This process is sometimes referred to as the *multilinear events sequencing technique*, and it provides the opportunity for a precede/follow logic check along both the horizontal time coordinate for a single participant, and along vertical coordinates for the sequencing of related events by two or more participants. In this manner, other participants can compare the timing of an event by a participant with any other event.

This approach provides a method for ‘‘proving’’ a hypothesis which differs from the standard statistical or experimental approaches of the scientific method. The multilinear events sequencing technique has the advantage of displaying unknown ‘‘linking’’ events in the sequence. It can also be used to develop new investigative leads which might otherwise not be considered.

A PREDICTIVE TECHNIQUE

This methodology can also be useful in the predictive study of property losses. For example, if a properly loss is viewed as one which would require more than one participant, the actions must occur in a specified chronological sequence to achieve a harmful outcome. If any of the events occurs out of sequence, or does not occur, the outcome being studied will not occur. This assumes that a recognizable and repeatable pattern of events is occurring in the first place. By altering the sequence of events through procedural changes or created checks, it is possible to prevent the loss from occurring. This technique not only applies to asset losses, but also to rare events such as industrial accidents or disasters.

Investigative Methods

The application of this technique requires a fundamental reassessment of the way in which most internal investigations are conducted. Data on loss events should be entered into a loss database for ready reference and study. A well-designed database will include fields for details of the loss event that will facilitate ready identification of loss patterns. Commercially available incident database software can usually be readily adapted for the needs of a particular enterprise. The data can be sorted in the form of *event sets*, rather than in the form of individual conditions or isolated events. The order in which the data can be sorted is usually limited only by the fields in the database. Sorting the events in chronological order by date, day of week or time of day is generally most helpful in analyzing the information. Sorting the event data by the persons involved, assets involved, sequential transaction numbers or the location from which the assets were taken are all useful. An analysis of the data will frequently readily identify the areas of greatest security vulnerability within a department and suggest appropriate changes. More important, the information can be presented in a way which is easily comprehended by management and which greatly enhances the success of the changes proposed by the security manager. Once management has embraced this concept, it is possible to estimate the probability of these events sets occurring, and the allocation of company resources for reducing the overall vulnerability can be established.

THE CRITICAL INCIDENT TECHNIQUE

Originally developed by the U.S. Military, the critical incident technique involved interviewing a large number of pilots and determining if they had ever made or seen anyone else make an error—no matter how minor—in reading or interpreting an aircraft instrument, detecting a signal or comprehending written or verbal instructions. In the course of this study, more than 270 ‘‘pilot error’’ incidents were identified, and many of those interviewed had reported almost identical experiences. This study led to a number of major aircraft design and procedural changes, which dramatically reduced the number of training accidents.

Variations of this same system have been tested in industrial accident research programs as well. A study of the usefulness of this technique as a method for identifying potential accident causes, and for developing procedures for its use in industry, produced the following findings:

- The critical incident technique dependably reveals causal factors in terms of errors and unsafe conditions which lead to industrial accidents.
- The technique is able to identify causal factors associated with both injury and non-injury accidents.

- The technique reveals a greater amount of information about accident causes than other methods of accident study, and provides a more sensitive measure of total accident performance.
- The causes of non-injury accidents, as identified by the critical incident technique, can be used to identify the source of potentially injurious accidents.
- Use of the critical incident technique to identify accident causes is feasible.

Applying the critical incident technique to the assets protection program can achieve a number of positive results, not the least of which is increased profitability. Rather than dealing with after-the-fact situations, the assets protection program can be integrated into the overall company planning process. Extending well beyond the historic features of security officers, fences, alarms and locks, it will become a rational attempt to integrate essential assets protection requirements in each step of the planning process.

An old security axiom holds that the most efficient work methods are inherently secure. For example, raw materials are usually the most vulnerable while in transit from one location to another. Therefore, conducting the least number of such movements is the most efficient and the most secure method, because the opportunities for diversions are minimized. But the proper design of workstations which include the means to secure tools, equipment and parts may result in a more efficient and secure than merely limiting movements. To be readily accepted by the workforce, however, any assets protection requirement must have the minimum possible negative effect on efficient operations.

The critical incident technique is based in large part upon the recalled experience of the people involved in the operation. It involves recalling those minor matters which can best be described as non-events—nothing actually happened, but the potential for a loss was present. Even getting employees to think about such matters will have a positive impact on the assets protection program. When employees perceive that line supervision and upper management are genuinely interested in improved security in their specific work area, security will almost always improve.

INTERVIEW TECHNIQUES

Experience has shown that two types of critical incident technique interviewing systems, formal and informal, can be utilized. Both types of interviews have significant value in improving the assets protection program. The planned or formal interview will generally produce the best results in terms of the number of events reported. But this is more time-consuming and requires some formal training for supervisors conducting such interviews. It may be worthwhile to start a critical incident technique interview program in this manner and then make the transition to a more informal method in which the supervisor routinely encourages the reporting of minor events by individual employees on a regular basis. This can be included as part of the normal production group meetings where supervisors discuss general work-related problems.

The major difference is that supervisors will be frankly discussing assets protection related matters as part of the normal work agenda and encouraging the workers to recommend improvements. In many cases, these discussions will be a new experience for the supervisor. Note that the emphasis is upon improving work methods while taking assets protection into consideration. It is not intended to become a mechanism to solicit employees to inform on one another.

The planned critical incident recall interview requires the supervisor to take the time to utilize a special interviewing technique with employees. The success of recall in terms of the number of events reported is directly related to the proficiency with which the supervisor conducts the interview. Properly administered, a system utilizing the planned interview technique will consistently reveal a larger number of events with a property loss potential than those obtained through more informal interview methods which rely heavily upon voluntary contributions by individual employees. The purpose of the planned interview is to get employees to focus on assets protection related issues and to consider those aspects of their functions which have a loss potential, no matter how minor it may seem to be.

The ability of the supervisor to elicit information is critical to the success of formal interviews. Note that in a group setting employees may be reluctant to be the first to provide information, even if directly questioned. A phenomenon known as *Groupthink* may also come into play. This is a condition in which participants give answers that conform to the perceived thoughts of the other participants rather than expressing their own thoughts.

Properly conducted, the planned interview can also be an effective learning device for the supervisor. Many other concerns and interests of the individual worker will be revealed during these interviews and it will be an ongoing learning process on both sides. The many small ‘‘housekeeping issues’’ that can weaken the most elaborate assets protection systems can be addressed at the work unit level in a timely and effective manner with little or no additional cost to the company. These minor changes will often contribute to improved morale and productivity as well.

Still, the informal interview method should not be ignored. The basic idea of a critical incident recall program is to encourage employees to recognize and report ongoing problems as they occur. The workplace is dynamic and is constantly undergoing minor changes. Many of these changes will have an impact on the assets protection program. The alert employee who believes the supervisor is interested in such matters will bring them to the supervisor’s attention on a frequent basis. Also, supervisors quickly discover that asking for brief reports of minor events with property loss potential at the close of the regular group meetings becomes an excellent stimulator for continued recognition and reporting of matters with an assets protection implication.

The effective supervisor keeps such event reports brief and makes sure that any comments from employees are always directed in a positive way to reinforce a desired behavior pattern. Emphasizing what was done to change reported conditions is one of the best ways to accomplish this. The regularity with which this practice is followed becomes a key to success in continuing to obtain such reports. The follow-up action taken by the supervisor should be reported back to the group at subsequent meetings with appropriate recognition to the employee who initially reported the event.

Other supervisors may prefer to close each personal contact with an employee by inviting the person to comment on assets protection related events in the work area. By making this practice a routine habit, many events become known that would not otherwise be reported, and corrective action can be taken. This personal approach has particular appeal to an employee who is easily embarrassed or reluctant to speak before a group.

In some cases, it may even be appropriate for the supervisor to designate an individual to be the assets protection event observer for a stipulated period of time. It would be the function of this employee to discuss with the supervisor any substandard working conditions or practices within the group which have a property loss potential. Rotating this assignment within the work group maintains the level of interest and provides another method of continuous security training.

It is important that the assets protection organization not view problems identified through these formal and informal interview techniques as criticisms of the security function. The program is really a form of feedback to help the assets protection organization spot problems sooner. For this reason, it is more reinforcing and supportive than critical. Occasional pinpointing of individual faults or errors is inevitable, but with skillful supervisory interview control, these can be approached more as process problems than individual criticisms. When the data have been made available to the assets protection function, further care can be exercised to purge personal items before taking further action.

Regardless of the techniques employed, the three most important practices by the supervisor to stimulate the employee's desire to voluntarily report such security incidents on a continuing basis are:

- The frequency of communications which encourage such reporting;
- The immediate behavior recognition of those who report security events; and
- Prompt effective supervisory action to control their recurrence.

DEVELOPING POSITIVE SECURITY CONTACTS

The success of the analytical techniques discussed in this chapter depends heavily on the support and cooperation of employees. The assets protection organization can facilitate cooperation by the employees in this effort by encouraging positive security contacts at all levels. This does not mean that the basic security mission is to be diminished or de-emphasized. Rather, it means that sincere efforts should be made to promote other types of associations or contacts with employees. A positive attitude toward the assets protection can be encouraged through measures to promote the personal safety and security of the employees and their families in the workplace and in other venues. Examples of such measures are:

- Conducting home protection clinics;
- Providing property-marking devices on a loan basis;
- Offering group purchase opportunities for burglary and fire protection devices;
- Conducting personal protection programs; and
- Conducting children's fire prevention poster campaigns with cash prizes.

Comments made by employees in the course of the interviews may suggest additional personal or properly protection programs that are of interest to the employee population.

SUMMARY

The process of security vulnerability assessment is frequently addressed as a program of physical security evaluation. In truth, the human element is a vital part of the process and can be of greater importance than the physical element. A cooperative employee who is concerned about the protection of the assets of the enterprise is far less likely to attempt to circumvent a physical or administrative feature of the assets protection program. Once employees understand that they have a stake in the success of the program, its ultimate success is much more likely.

SELECTED BIBLIOGRAPHY BOOKS

Dalton, Dennis; *The Art of Successful Security Management*; 1998, Butterworth-Heinemann, Newton, MA.

D'Addario, Francis J.; *Loss Prevention Through Crime Analysis*; 1989, Butterworth-Heinemann, Newton, MA.

Higgins, Clay E.; *Applied Security Management*; 1991, Charles C. Thomas Publishers, Springfield, IL.

Purpura, Philip P.; *Security and Loss Prevention: An Introduction; Third Edition*; 1998, Butterworth-Heinemann, Newton, MA.

ARTICLES

Security Management, American Society for Industrial Security, Alexandria, VA.

—Cottringer, William S.; *Communicating Wisely and Well*; 12/95.

—Detore, John A.; *Spreading Security's Good Word*; 11/97.

—Goldberg, Joel A.; *Security's Challenges: A Roundtable Discussion*; 7/94.

—Okun, Martin J., CPP and Hocking, William T; *Living Through Empowerment*; 11/97.

—Pennings, Bruce W.; *Committee in the Rye*; 7/96.

—*Shaping Attitudes: A New Approach to Loss Prevention*; 1/83.

—Sutherland, Garrell E.; *Answering the Question—What is Security?*; 7/92.

Security Technology and Design, Locksmith Publishing Corp., Park Ridge, IL.

—Read Hayes, CPP, CST; *Crime and Loss Control Training*, 3/98.

—Read Hayes, CPP, CST; *The Four As: Shrinkage Can Be Controlled*; 3/97.

APPENDIX A

SUPERVISOR'S GUIDE FOR CONDUCTING THE PLANNED CRITICAL INCIDENT RECALL INTERVIEW

General

The basic objective of the planned incident recall interview is to gain the willing cooperation of employees, so that they will feel free to relate all security events with a property loss potential that can be recalled. The events reported do not have to be confined to a given time span and, oftentimes, the most lasting memories may have been of events which occurred months or years before. While it is important to relate them to a specific time frame, it does not necessarily follow that old events do not have relevance to current problems. Since the success or failure of the critical incident recall program depends upon the results of the employee interviews, it is important for the supervisor to have an understanding of good interviewing techniques and practices.

Background

First-line supervisors are the most qualified to interview employees under their supervision whenever a planned program of critical incident recall is initiated. While supervisors may not have the special knowledge and experience of the security professional, they are not considered to be outsiders by the average employee and are better able to relate to the matters under discussion. In addition, line supervisors often have the means under their immediate control to effect a work change as a result of the employee's suggestion. This sense of an immediate report—change effect will encourage others to think about other security-related matters at their work station as well. Most supervisors:

- Have a personal interest to protect, since it is their work unit which is under observation;
- Know the most about the employees and conditions in the work area;
- Know how to get the information and evaluate its relevance; and
- Will take the appropriate action.

Many employees have been conditioned to associate blame fixing and faultfinding with the reporting of security events. This well-founded association is one of the major reasons why many security matters go unreported, or why there is a significant lag in the reporting time in relation to the event. The planned critical incident recall interview must be conducted with a no-fault, no-discipline assurance to all participants. The emphasis must be upon identifying workplace conditions and practices rather than finger pointing. The use of informants has no place in a critical incident recall interview program.

Procedure

1. Put the employee at ease by being friendly and sincere. One of the best ways to create favorable rapport for a good recall interview is to talk briefly about the employee's family or a subject which is of particular interest. This step appeals to the basic psychological needs of the average employee and provides the necessary motivation which will insure cooperation.
2. Explain the purpose for the interview and the importance of personal recall. Try to create a desire on the part of the employee to participate in a program which will enhance the security of the workplace.
3. Give assurance that the recall interview will be kept confidential. The degree to which recall is achieved is often related to the success of the supervisor's ability to convince the employee that the interview is privileged. It should be emphasized that the only purpose of recall is to identify events with a potential for property loss and not to comment upon the actions of other employees.
4. Point out that recall benefits everyone—the company, the department and the employee. Anything that contributes to the efficiency and profitability of the company will help everyone.
5. Ask employees to recall each event they can remember seeing or hearing about that, under slightly different circumstances, could have resulted in a serious property loss. With each incident recalled, be sure to determine how many times the event may have occurred in a given time span. This information will help to determine the probable rate of recurrence and serve as a guide to the urgency and extent of any action necessary. Explain that the purpose of the interview is not to determine why it happened or what to do about it.
6. Ask questions to fill in any gaps in the employee's narrative, but try to avoid interrupting the employee's train of thought in the process. The best method is to let employees tell the complete story in their own way, and then follow up with pertinent questions.
7. Review your understanding of the event with employees. Quickly repeat your understanding of each event in order to make sure the information is accurate.
8. Discuss causes and remedies if time permits. Invite the employee's opinion on the possible causes as well as any suggested remedies or controls. If any follow-up action is required or anticipated, be sure to set a time when you will get back to the employee with the outcome.
9. Express your sincere thanks for the employee's cooperation.

APPENDIX B

MODEL TEAM MEETING NOTICE

From: (Name), Team Leader.

To: All permanent team members and any temporary members required for the session.

Subject: Vulnerability Assessment Team Meeting

Reference is made to the policy letter of the *CEO* or *COO* dated ________________.

As required by the policy letter, the first meeting of the vulnerability assessment team has been scheduled for (*date, about a month after the notice letter*).

The activity which has been selected for review at the first session is (*identify the activity*).

(*add if appropriate*) As this activity is not represented by a permanent team member, (*name the responsible manager*) has been invited to participate in this review session as a temporary team member.

The team will meet at (*location*) commencing at (*hour*) on (*date*). The luncheon break will be from (*time to time*) and luncheon will be provided for the members.

Attached to this notice are (*representative loss scenarios, copies of relevant procedure, or other appropriate enclosures*). All addressees are requested to familiarize themselves with the attachments and to review their usual role in the activity under review, prior to the meeting date. Addressees are also requested to acknowledge this notice. Any questions may be directed to undersigned at (*telephone extension*).

It is anticipated that the scheduled meeting will require the entire day[1] and addressees are requested to adjust their calendars accordingly. If any addressee foresees an urgent reason why attendance will not be possible, it is requested that a responsible alternate be designated and that the undersigned be notified promptly.

Signed,
(Name)
Team Leader

encls:

[1] Depending on the management style of the organization, it may be better to schedule more but shorter meetings.