U.S. Department of Justice
National Institute of Justice

CRIMINAL JUSTICE BOOK SUMMARIES

a service provided by the National Institute of Justice/National Criminal Justice Reference Service

Risk Analysis and the Security Survey

by James F. Broder

According to studies by the National Science Foundation and independent insurance companies, the estimated annual property damage in the United States due to natural hazard exceeds $6.2 billion. Losses due to white collar crime alone are estimated in the range of $40 to $60 billion per year. These statistics do not assess the loss of human life or price of suffering, nor the price society pays because of such crime.

Risk Analysis and the Security Survey discusses these and other issues surrounding the need to protect assets and resources. The author offers theoretical, conceptual, and practical information for the working security practitioner, student, and security consultant who conducts security surveys and audits.

Risk and security management are concerned with the protection and conservation of corporate assets and resources. Corporations use risk and security management to first prevent loss and then to minimize loss when an emergency situation occurs or disaster strikes.

One of the security manager's main tasks is to collect accurate and detailed information about what risks exist. Once the risks are identified, the manager can evaluate and develop loss control measures using a three-part approach:

1. Implement sound security procedures to minimize the probability that a disaster will occur.
2. Design plans to minimize the loss or damage if a disaster does occur.
3. Develop and update disaster recovery plans and procedures to ensure that the facility is able to recover quickly and remain in business.

The most fundamental principle of risk control, design, and implementation is that the security program be as self-sufficient as possible. The system should (1) protect assets by identifying and analyzing the risk and (2) provide for disaster recovery.

Risk Analysis and the Security Survey is divided into four broad subject areas: survey techniques, insurance requirements, program development, and operational activities. The following sections summarize the author's presentation on each subject area.

Definition of terms

Risk is the uncertainty of financial loss, the variations between actual and expected results, or the probability that a loss has occurred or will occur. The three categories of risk are: (1) people assets, (2) material assets, and (3) liability. **Perils** are the causes of risk (e.g., fire, flood, earthquake). **Hazards** are factors that contribute to perils (e.g., a loaded gun, a pile of oily rags).

Risk analysis is a thoughtful and orderly method for estimating the anticipated or expected loss from the occurrence of some adverse event. It should be performed periodically to assess changes in a company's mission, facilities, and equipment and strike a balance between the impact of the risk involved and the cost of taking protective measures.

The first step in an analysis of risk is to identify types of loss (such as fire, robbery, kidnapping) and their effect, to estimate the probability of occurrence, and to measure the impact or severity of the risk.

Identifying risk

Identifying risk involves several basic considerations:

- Assets—What does the company own, operate, lease, control, have

Summarized from *Risk Analysis and the Security Survey* NCJ 93429 by James F. Broder with permission from Butterworth Publishers. 1984. Summary published February 1986.

Risk Analysis and the Security Survey is available from Butterworth Publishers, 80 Montvale Avenue, Stoneham, MA 02180. Price $22.95

custody of or responsibility for, buy, sell, service, design, produce, manufacture, test, analyze, or maintain?

- Exposure—What is the company exposed to that could cause or contribute to damage, theft, or loss of company assets or that could cause or contribute to personal injury?

- Losses—What empirical knowledge is available to identify the frequency, magnitude, and range of past losses experienced by this and similar companies performing a like service or manufacturing a similar product?

A general security checklist will include many items that are appropriate in some situations but not in others. The checklist may contain a review of policy and programs, the number and type of security personnel, barriers (fences, gates, walls), alarms, lighting, the means of entering and moving about the building, type of property control, emergency planning, and personnel screening.

Measuring risk

The total cost of an adverse event can be mathematically calculated by adding the cost of the event plus the frequency with which it may occur. (The text provides charts and probability tables to determine the impact in dollars.)

Statistical analysis and procedures can help in designing a security system that reduces the ratio of unfavorable events. But no statistical procedure can, in itself, ensure against mistakes, inaccuracies, faulty reasoning, or incorrect conclusions. Analysis is useful only if the data are accurate, the methods properly applied, and the results interpreted by someone who has a thorough understanding of the field in which they are applied.

Measuring risk involves a series of interrelated tasks that can be especially difficult if the necessary information is insufficient; but adequate estimates of the potential dollar loss are essential if the analysis is to be accurate.

One technique for measuring security needs involves reviewing methods for prevention, control, and recovery. Prevention attempts to stop security incidents before they get started; control attempts to minimize loss and to keep security incidents from affecting assets; recovery restores the operation after assets have been adversely affected.

Another technique for assessing security is to prepare a schedule of overhead, installation, and operating costs for the security project. In this process, it is essential to show that benefits will outweigh costs.

Some evaluators measure loss potential by using a decision matrix. The matrix should take into consideration the available sources of information, the probability that certain relationships will occur, the minimum time and resources required, maximum incentive for management cooperation, and a realistic evaluation of the effectiveness of the existing or planned security system.

Designing a cost-effective system

Several techniques can be used to design cost-effective security systems: (1) design the system to suit the environment, (2) build redundancy into the system, and (3) prepare security countermeasures. A survey of the project's needs is a fundamental first step regardless of which technique the security manager chooses.

The security survey

The security survey is a critical, onsite examination and analysis of the project's needs. It is designed to reduce incidents that lead to loss. The survey can establish if a company's risk reduction plan is adequate. If the company has no plan, it can be the basis for establishing a need and then developing one.

The basic purpose of the preliminary survey is to get an indepth overview of the operation. A good preliminary survey may even substitute for many parts of the final examination.

About 50 percent of the survey is done in the field, about 25 percent is devoted to planning the survey, and 25 percent to writing the final report.

Field work measures data, records, and procedures that may have an effect on the operation. It involves observing, questioning, analyzing, verifying, investigating, and evaluating. It begins with an interview with department heads to obtain information on documentation of the company's policies, financial reports, problem areas, and other matters of special interest.

Some managers have no idea what kind of security they need or how much loss is attributable to theft by unauthorized personnel and visitors. Some managers, for a variety of reasons, are reluctant to discuss the subject of security, and they must be convinced that security is worth the price. There are a number of actions security professionals can take to alleviate these potential problems:

- establish a meaningful dialog with the decisionmakers;
- deal in principles, not personalities, and maintain an objective view;
- be as well informed about security as possible and present information in a timely fashion;
- present proposals as briefly as possible;
- suggest that management obtain a second opinion from an outside consultant;
- develop a promotional program to ensure that the system is successfully implemented within the company.

The survey report

A well-written report communicates and persuades in an accurate, clear, concise, and timely manner. The form is dictated by its audience, by the writer's preference, or by the type of report (formal or informal, final or interim, written or oral). It should be accompanied by a one-page cover letter. The following elements are common:

- a title with the date of the survey;
- an introduction or foreword that briefly describes the purpose of the study;
- a brief description of the objectives of the survey;
- a statement of the scope of the survey;

- the findings—the product of the reviews, examinations, observations, analyses, and investigations; and
- a brief conclusion stating the opinion and professional judgment of the person making the review.

Insurance requirements

Risk management is the process for identifying potential losses, and selecting treatment of these potential losses. Three types of risk management are possible: (1) avoid, eliminate, or reduce the risk, (2) assume or retain the risk, (3) transfer the risk to a third party.

Crime insurance usually supplements the security program by reimbursing the company for losses. Minimum crime insurance will usually reimburse a company for losses due to dishonesty, disappearance, and destruction. Specialized crime insurance is also available, but prevention is the best insurance.

Basic kidnap and ransom (K&R) coverage provides reimbursement for loss of moneys surrendered as a ransom payment and for related costs in property, time loss, and so forth.

Establishing a disaster recovery plan

Industry and government share responsibility for protecting lives and property. Preparedness helps avoid loss and assures continuity of production. Coordination of all emergency operations is essential to preparedness. Emergency operations include the regular police and security forces, fire forces, ambulances, hospitals, and medical personnel, and all other people and units with capabilities for helping under disaster conditions.

The essential first step in preparing for disaster operations is to establish an overall corporate disaster plan that has the approval of management as well as appropriate government officials. Appointing an emergency coordinator who is trained in emergency management can facilitate operation of the plan.

A basic disaster plan should include the following elements:

- establish a place that can be used as an emergency control center;
- list the types of emergencies that are most likely to affect the plant;
- describe the coordination of company actions before and during a disaster;
- develop emergency shutdown procedures;
- keep employees informed of the plan;
- keep the roster of disaster workers current.

Contingency planning

Contingency planning involves writing a systematic plan to reduce the impact of events having the potential for large losses (such as fire, explosion, flood, earthquake, or tornado). Developing a contingency plan hinges on the same steps as a disaster plan:

- organize and administer the risk management function;
- identify resources that are exposed to accidental loss;
- evaluate the risks to which the resources are exposed;
- develop programs that control the risk;
- finance the cost of the expected loss.

Rarely are contingency plans systematically developed before they are put into operation. Most plans are developed on a hit-or-miss basis, receive little inspection, review, or audit by management, and are not tested before they are needed.

Crisis management planning

A crisis management team can prepare a readiness plan to minimize potential losses due to executive kidnapping and terrorism. The team usually consists of a small number of senior personnel who make corporate decisions when data and time are limited and lives are threatened.

The first crucial moments of a crisis situation may determine the final outcome. Goals should be to calm the extortionist, secure proof that the hostage is being held unharmed, enact a prearranged code, bargain for time, and provide for additional contacts. Decisions about paying the ransom will have to be made in the early phases of the crisis.

Like other types of risk, prevention is important. Prevention includes making the physical environment secure, instructing children of potential victims on precautions, and limiting dissemination of personal information about potential victims.

Generally, individuals who are kidnapped should not jeopardize the abductors' plan. They should convince their captors that their well-being is essential to a successful operation, and become a "person," not an object. The individual should give maximum information to the crisis management team through prearranged codes. Escape should be considered only as a last resort when death appears to be the only likely alternative.

Monitoring safeguards

In sharp contrast to the methods used in the scientific and engineering fields where testing is routine, testing security safeguards and countermeasures is probably the one critical area most likely to be overlooked.

Testing evaluates performance and reveals weakness, failure, or potential flaws in the system. It has a specified objective and may apply to persons, systems, procedures, methodology, or objects.

Routine testing is both time consuming and costly, but can be reduced by using basic audit techniques (limiting the number of test cases to a statistical sample), limiting the scope or field of inquiry, and scheduling the testing over a period of time.

Management, however, should be aware that every test shortcut has its price in terms of the potential risk.

The security consultant

The independent professional has only one loyalty—the best interests of the client. He or she can be impartial to

the internal politics. But employees sometimes regard a consultant as an outsider, an interloper, a stranger, one who has no real feeling for the company or its employees, but who is paid very high fees. Consultants are able to complete their work more effectively if they are sensitive to the potentially negative reaction employees may have.

In-house security professionals are often already fully employed at the day-to-day operation of the company and lack the time to conduct a professional security survey. In-house staff may also be unaware of the latest techniques and developments since most people concentrate on their own sphere of activity. Management may find that a consultant who has worked on several different types of security systems brings a fresh insight to the operation and may be worth considering.

Sources on this topic

American Society for Industrial Security
Sara Dowdey, Information Specialist
1655 North Ft. Meyer Drive, Suite 1200
Arlington, VA 22209
703–522–5800
Responds to written requests for information; answers specific inquiries by telephone; provides prepared reports and reprints of articles from *Security Management Magazine*.

Further readings

Security Design for Maximum Protection. NCJ 93549. By R.J. Gigliotti and R.C. Jason. Butterworth Publishers, 80 Montvale Avenue, Stoneham, MA 12180. 1984. 352 pp. $34.95.

A Re-Evaluation of Crime Prevention Through Environmental Design in Portland, Oregon: An Executive Summary. NCJ 80573. By J. Kushmuck and S. Whittemore. Sponsored by the National Institute of Justice. 1981. 49 pp. Availability: NCJRS (free).

Commercial Security Field Test Program: Impact of Security Surveys on Commercial Crime, Executive Summary. NCJ 97519. By J. Tien and M. Cann. Sponsored by the National Institute of Justice. 1984. 34 pp. Availability: NCJRS sales document. Price: $8.40.

Security Letter
Robert McCrie
166 East 96th Street
New York, NY 10028
212–348–1553
Responds to written requests for information; answers specific inquiries by telephone; provides referrals to other information sources.

International Association of Professional Security Consultants
Scott Roulston
P.O. Box 93941
Cleveland, OH 44101
216–881–1200
Responds to written requests for information; answers specific inquiries by telephone; provides a free directory of security consultants.