HARRINGTON GROUP
Asset Protection Solutions

***Eternal vigilance is the price of liberty.***

– Wendell Phillips

***That much gathers more is true on every plane of existence and that loss leads to greater loss is equally true.***

– Charles F. Haanel

**White Paper - Asset Protection Management**

**CONTENTS:**



## The Management Function

Protecting the assets of any corporation, institution or public interest today is a daunting task. The role of the loss prevention/assets protection professional is rapidly changing in this environment and requires a combination of strategic thinking, process management and the ability to implement programs and initiatives in increasingly shorter periods of time to match the incredible pace of today's business.

Macroeconomics teaches us that resources in any given situation are limited; thus, choices must be made regarding the trade-off between the resources necessary to generate products, profits and market share, and the assets required to secure and protect them. The successful assets protection professional strikes the appropriate balance between these competing demands. It is the goal of the **H**arrington **G**roup **A**sset **P**rotection **S**olutions (HGAPS) to assist the loss prevention/assets protection professional in achieving this difficult but essential equilibrium in determining the appropriate level of acceptable risk/loss in any given situation and the investment required to mitigate those risks/losses.


**Joseph E. Harrington, Ph.D. • 2110 Artesia Blvd., Suite #610 • Redondo Beach • California • 90278**
**Tel: 310-376-4277 (GAPS) • Fax: 310-391-6700**
**Joseph@HGAPS.com • www.HGAPS.com**

**A Historical Perspective**

From the earliest of times, humans have recognized the need to protect themselves, their family and their property/assets. Individuals or small groups living together provided the protection until loosely organized tribes developed into more formal groups. As civilization began to trace outlines of government in the sense that we would recognize it today, the need for forces to maintain order was acknowledged. These forces were usually created to deal with the threat of attack from other groups and not with problems of order within the primary group itself. The raising of armies and their deployment to territorial borders was the initial method of establishing group defense and protection.

As local communities were further removed from the seat of central power and as more individuals in those communities were strangers to each other, rather than close relatives, the need became clear for some form of local order and control. This was done to preserve peace and enforce laws made at distant regional or central capitals. Primitive forms of night watch and patrol were developed, again to protect the community against outside attack. The idea of public protection for private property did not take hold until after the industrial revolution and even today is a concept of limited application. The proprietor of a private enterprise or the owner of private assets is and always has been largely responsible and self-dependent for adequate protection against all but major threats to the public peace and financial peace of mind.

The hazards faced by every industrial and business enterprise, as well as by private and public institutions, have continued to multiply over the years. There is ample anecdotal evidence that the viability of the enterprise is frequently threatened by the loss of financial, human and physical assets. As a result, the protection of the assets of every organization has continued to increase in importance, and the protection field has become more and more sophisticated. There are new sets of skills and tools required in the protection of assets in the new millennium.

For that very reason, the **H**arrington **G**roup **A**sset **P**rotection **S**olutions created HGAPS: an online national database and clearinghouse. We developed asset protection tools and materials. We also formed strategic alliances with industry associations, law enforcement and private investigators to offer the full range of functions required to protect the modern enterprise from losses.

**Definition of Assets Protection**

Generally, we consider money, accounts receivable, physical property, intellectual property and proprietary information as assets. But employees of the enterprise may also be considered among the most valuable assets. Without a skilled workforce, other assets may be useless in accomplishing business purposes.

The hazards to be considered and faced by every organization when designing an assets protection management program may be divided into two classes of individuals:

- Those who have a right or license to be inside the organization or facility, such as employees, contractors, temporary employees, visitors and customers.

- Outsiders who intend to cause harm, such as thieves, burglars, robbers, and vandals, whether their intention is to enter the facility physically or divert assets through a conspiracy between inside employees, customers, distributors, vendors/suppliers and delivery drivers.

Losses resulting from the misbehavior of people, both inside and outside the enterprise, can have a broad range of causes. Some of the more common are:

- Waste, Variability, and Inflexibility

- Decision-Making mistakes

- Dishonesty

- Theft of company property/assets
- Fraud and conflict of interest, which are destructive to the interrelationships of employees, organizational trust and potentially the reputation of employees and the firm itself.
- Sabotage, criminal damage, etc.
- Extortion
- Maliciously willful or negligent personal conduct
- Unprofitable Habits

**Basic Considerations**

There are two factors that determine the quality of an assets protection management program:

- An adequate and active prevention plan to track, account, and limit losses.
- Top management's understanding and support of the program.

**Countermeasures Planning**

Rather than formulate and implement a comprehensive asset prevention plan, some organizations adopt asset protection measures in bits and pieces, reacting to problems as they occur. In fact, in some cases the problems are avoided until they become so serious that they can no longer be ignored. With a proactive effort, a complete plan could be developed to include all types of solutions and measures, instead of coping with only one risk/loss situation.

Avoidance of loss or prevention of loss is important in the design of the complete plan. Some security and protection programs have been based almost entirely on after-the-fact responses to events that have already occurred. This is appropriately described as "crisis management." An example is the enterprise that depends entirely upon arrest and prosecution to deter dishonesty, theft and extortion. While fear of detection will discourage some individuals, others will conclude that the risk of discovery is small and they will take a chance.

When a loss does occur, every organization has the right to make a criminal complaint and to initiate civil action to recover damages, when appropriate. The goal of the criminal complaint is a conviction with an order of restitution. In a civil action, judgment for the organization will result in an order for restitution. But those orders may be of little economic value if it is impossible to recover anything. This often happens, and firms have been forced out of business because they were unable to recover their losses. The fact that an individual is convicted and sentenced to jail will be of little benefit to an organization that has been damaged. This explains why *private security is more interested in loss prevention than in loss detection and prosecution.*

**H**arrington **G**roup **A**sset **P**rotection **S**olutions (HGAPS) believes that many potential losses can be avoided by unification, accurate data, communication, effective decision-making, security and assets protection controls across the entire flow lines.

**Management Support**

Some assets protection programs have been ineffective because the second basic factor, the need for ***complete management support***, has not been efficiently stressed. When senior management delegates complete assets protection responsibility to lower-level managers without top-level backing, the results are usually unsatisfactory. The assets protection program must be fully understood and supported at the top level in the enterprise and senior management must be interested enough to ensure that all personnel follow the established requirements.

The example, good or bad, set by senior executives in complying with requirements will permeate the organization. It is incumbent upon the asset protection professional to establish a well-defined strategy and communications program to ensure all levels of management and employees understand the goals of the assets protection management program.

Neglect or a lack of appreciation for adequate assets protection can also result in personal liability for corporate officers and directors – the stockholder's suit. Top officials of a company may be personally involved in legal actions if stockholders become aware of losses that could have been prevented by a prudent assets protection program.

Businesses that have an assets protection compliance program designed to deter and detect criminal conduct can result in a significant reduction in risk/loss. Therefore:

1. The company must establish compliance standards that are reasonably capable of preventing criminal conduct.

2. High-level management must have specific responsibility to oversee the standards.

3. The standards must be communicated to the employees and training in compliance issues should be offered.

4. The company should test the system by monitoring, auditing and other systems designed to detect criminal conduct.

5. The company must exercise due care to ensure that discretionary authority is not delegated to individuals with a propensity to engage in illegality.

6. The compliance standards must be enforced through appropriate disciplinary procedures that include provisions that those individuals will be disciplined for failing to detect or report an offence.

7. After an offense is detected, all reasonable steps must be taken to prevent a future similar offence.

**Communicating the Plan**

Top management support of the plan will be based on a solid understanding of the value of the effort. The plan must, therefore, be couched in terms that will be readily understood by top management. Business is ultimately conducted in financial terms and the prudent assets protection professional will communicate in those terms. Senior management will usually embrace an assets protection plan that is cost-effective and, if possible, provides a return on the investment made.

The innovative assets protection professional will meet the requirements in a cost-effective manner and, where possible, simultaneously fulfill other risk/loss needs of the enterprise.

**The Systems Approach**

To be effective, the design and implementation of an assets protection management program incorporates the systems approach, defined as a ***comprehensive solution to a total problem***. This is an orderly and rational method of problem solving and, when properly carried out, should ensure a sound program.

1. A vulnerability/loss analysis.

2. Selection and installation of countermeasures.

3. A thorough test and analysis of the operating system, management infrastructure, mindsets, capabilities and behaviors.

**Vulnerability/Loss**

A basic precept of assets protection is that an *effective program must be based on a clear understanding of the actual risks/losses it faced.* Until the actual threat to assets is assessed accurately, precautions and countermeasures – even those of the highest quality, reliability and repute – cannot be chosen, except by guesswork. The value of the assets protection program depends as much upon the relevance of resources as upon their high quality. ***First*** understand the problem; ***then*** consider solutions.

Defining an assets risk/loss problem involves an accurate assessment of three factors:

1. The kinds of threats or risks affecting the assets to be safeguarded.

2. The probability of those threats becoming actual loss events.

3. The effect on the assets or on the enterprise responsible for the assets if the loss occurs.

The first can be called *loss event profile*, the second *loss event probability* or *frequency*, and the third *loss event criticality*.

The relationship among these three aspects of a loss event is fundamental in any system of countermeasures. Each aspect increases or decreases in significance in the light of the other aspects. For example, if a loss event probability or frequency is high, then even relatively low loss event criticality becomes significant because of the probable repeated events. A single loss event with criticality that, considered alone, would have only a slight impact would require different assessment if that loss event were to occur hundreds, thousands or millions of times in any one year.

A security and assets protection countermeasure should be planned if the loss event has the following characteristics:

- The event will produce an actual loss, measurable in some standard medium such as dollars.

- The loss is not speculative in the sense that nonoccurrence of the event would result in a gain.

The kind of event that may produce either a loss or a gain is often called a business or conventional risk. To the extent that these assets are properly managed and protected, sales are profitable. Loss results from failure to manage and protect them correctly. Properly gauging the profit and loss potential is the task of conventional business management.

But if the anticipated profit were not realized because of some event that could only cause a loss, the situation would call for positive assets protection and loss prevention measures. A professional assessment is necessary if countermeasures planning are to have any value.

**Countermeasures**

Countermeasures apply to people, hardware and software. All three must be interrelated in the system design to ensure an effective, integrated asset protection program. For the purposes of this discussion, the term “software,” in addition to electronic systems programming instructions, will refer to all directives and instructional or training material, written and verbal, needed to make an assets protection program operate as intended.

**People**

People are the most important and generally the most expensive of the three types of countermeasures. During system design, particular attention should be given to the substitution of automated functions for people wherever possible and to deriving optimal return on the investment when people must be used. This is referred to as shifting from a *labor-intensive* to a *capital-intensive* approach.

For maximum efficiency, assets protection procedures can specify that operating employees and managers in areas other than assets protection perform certain assets protection checks and controls as part of their own regular duties. Loss prevention and assets protection personnel can conduct spot-checks or detailed inspections to ensure that the operating personnel are performing the functions assigned to them. In an automated environment, the performance of some of the checks can be reported electronically to the assets protection control system.

Loss prevention and assets protection personnel may be employees of the enterprise or contract employees, or a combination. Organizations of sufficient size normally assign responsibility for administration of the program to a full-time executive. This official usually has a number of employees and may have, in addition, contract personnel such as consultants and security officers. Smaller organizations, not able to justify the cost of a full-time executive for the loss prevention and assets protection function, may rely on other employees to administer the program on a part-time or added-duty basis. In such situations, contract personnel can be utilized extensively. The current trend in both large and small organizations is to outsource many of the loss prevention and assets protection management functions that have historically been performed by company employees.

Regardless of whether the enterprise is large or small, it is essential that a skilled administrator be delegated the authority and direct responsibility for the assets protection program on at least a part-time basis. The individual selected should be of sufficient stature in the organization to operate as an acknowledged member of responsible management. Some organizations make the mistake of assigning this task to an individual with limited supervisory skill and management experience. When this is done, the assets protection program will almost certainly be less than optimal; it may even fail, mainly due to a lack of executive access by the assigned individual.

If contract assets protection service personnel are utilized, the contribution each service provider will make to the complete assets protection system must be carefully assessed. They must be able to recommend practical and cost-effective solutions to the complete assets protection problem.

**Hardware**

Some examples of hardware items (the second element of countermeasures) are locks, fencing, lights, closed-circuit television and other electronic devices. When properly utilized, these can make a significant contribution to the protection of assets. As with the other two countermeasures categories, people and software, each item of hardware must be carefully planned to ensure that it interrelates with the system and economically increases the protection of the assets.

A lock, for instance, has traditionally been regarded as an effective security measure; however, a lock should not be expected to provide complete assets protection. A door or fence secured by a lock might be penetrated without ever touching the lock by using a pry bar or jimmy, or by cutting the latch bolt with a torch or saw. To make a lock effective, procedures should be established defining how and when it is to be used, to arrange for a periodic inspection by the individual in charge, and to provide detection and adequate response in case of penetration. So planned, all three countermeasure categories are involved. A lock is the hardware element. Software is represented by procedures providing for the activation, inspection and response to risk/loss. And the third element, people, is needed to inspect and respond in case a loss or penetration is signaled.

**Software**

In this discussion, the term “software” refers to electronic system programming instructions and to all directives and instructional or training material, written and verbal, needed to make an assets protection program operate as intended.

A basic item in any assets protection system is a written policy statement issued by the top management of the enterprise establishing the program. This statement, and others that may be released, set the tone and stage for the complete program, indicate the interest of top management and are the basis for implementing material.

Other procedures, practices and directives usually define in detail the controls that are being established throughout the enterprise and the responsibilities all employees must assume. Such material should be designed so that it can be easily understood and followed by employees at all levels in the organization. It is usually not adequate simply to issue directives or procedures and expect them to be followed without explanation.

The material should take into consideration that all employees in the organization must participate and assist in the assets protection program to make it operate successfully. It should be stressed to managers and supervisors at all levels that they must ensure the compliance of all employees under their supervision. The cooperation and assistance of all employees is necessary because the assets protection organization, regardless of its size, cannot protect the enterprise alone. Therefore, general employee reaction and attitude are important.

An assets protection program necessarily imposes controls and limits on people and their activities. A natural antagonism may develop if the program is not implemented properly. Employees resent controls that seem arbitrary; thus, the assets protection program should be designed for the least possible disruption of normal operations. If the need for controls, the benefits to the employees and the method of operation of the assets protection program are reasonably explained, most employees will accept the program and help make it work.

An educational effort reduces resistance and enhances cooperation. The educational effort should be implemented when planning for the assets protection program is started. This will reduce the normal human resistance to unexpected change. Employees should be advised, in positive manner, of the projected operational changes in the implementation of the assets protection program.

Employees are often not aware that losses must be deducted directly from the profits of the organization. They must be shown that losses that might at first appear very small could have far-reaching effects on profitability and might even have adverse effect on staffing. Employees can be informed that prevention of a loss will avoid a decrease in net profit, and that the success of the organization, largely measured in profit, will enhance personal security for them in terms of future employment.

Losses resulting from dishonesty, theft and extortion can also have a serious impact on profits. A $100 theft loss in a business earning a 2 percent net profit requires that sales increase $5000 to offset the loss. A 0.5 percent theft loss in a business with $100 million in sales at a 5 percent profit margin would require another $10 million in sales to offset it. Actually, losses are ***never*** really offset unless directly indemnified. No matter how much sales increase, the original loss remains.

Let me emphasize it again, employees take a greater interest in the assets protection program, and are more willing to make a contribution to its success, if they understand that the program has been designed for their own protection as well as the protection of the enterprise. The fact that a complete assets protection plan has been designed to cope with all types of risk/loss – should be explained. Employees need to be reminded of how the plan benefits them by safeguarding their financial lives and welfare.

In addition to policies, procedures and directives, a variety of other means can be utilized to inform employees of the operation of the assets protection program and the contributions they are expected to make to it. Some of the methods for instructing employees are:

- Publication of a assets protection manual
- Articles in the company newsletter
- Bulletins and posters
- Awareness presentations
- Discussions in staff or other types of meetings

Each organization will determine its own best means of communication with employees. The education process must be a continuing one so that employees are constantly reminded of the importance of the assets protection program.

Methods of dealing with employees who violate or ignore procedures must be established. Violation of an assets protection practice should be handled in the same way that the infraction of any other major company practice is handled. The problem should be referred to the appropriate level of supervision for corrective action. As part of the educational effort, employees and supervisors should be informed of the standards and procedures that have been established for addressing instances of nonconformance.

Once procedures or practices for use within the organization are developed, the managers and employees must be given appropriate instructions so they are familiar with the detailed operation of the assets protection program.

**The System Test**

For several reasons, tests of the operating program are essential in the implementation of the assets protection system. Tests should result in the following:

- Risks or loss still existing are identified and system deficiencies are revealed.
- System changes required to accommodate facility or organization revisions become apparent.

Checks or tests can be performed by the regular workforce as part of their normal work assignments, as well as by the employees operating the assets protection system. Arrangements should be made to test the system frequently and make necessary adjustments.

Selected employees can be asked to make suggestions for the improvement of the assets protection program. If the education effort mentioned earlier has been effective, the response will usually be positive. General employee comments and suggestions also give some indication of how well the assets protection system is operating and what changes, if any, should be made. The comments and suggestions will frequently involve modifications to make compliance with the assets protection program more convenient to the employees. If these suggestions can be implemented without sacrificing the security of the assets, the employees, feeling that they have contributed to the plan, will usually cooperate more readily with the assets protection program.

Procedures can be established requiring managers and supervisors at all levels to make regular checks to ensure that employees comply with the system requirements. Supervisory personnel can also be prepared to perform other tasks, such as inspections of areas and periodic audits of transactions, and to report any discrepancies to the executive responsible for the operation of the system.

**H**arrington **G**roup **A**sset **P**rotection **S**olutions (HGAPS) will remain alert to any deficiencies in the assets protection system operation. In addition, we can be assigned specific auditing and consulting responsibilities to be performed periodically.