PERIMETER SECURITY

- Plan and design protective barriers such as fences, gates, lighting systems
- Select the right intrusion detection system for securing all points of entry
- Conduct and evaluate risk and threat assessment
- Use downloadable checklists, forms, and questionnaires for a quick start to more secure built environments

Michael J. Arata, Jr.

Perimeter Security

Michael J. Arata, Jr.

McGraw-Hill
New York Chicago San Francisco Lisbon London Madrid
Mexico City Milan New Delhi San Juan Seoul
Singapore Sydney Toronto

The McGraw-Hill Companies

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 1 0 9 8 7 6 5

ISBN 0-07-146028-4

The sponsoring editor for this book was Larry S. Hager and the production supervisor was Pamela A. Pelton. It was set in Bembo by Lone Wolf Enterprises, Ltd. The art director for the cover was Anthony Landi.

Printed and bound by RR Donnelley.

This book is printed on recycled, acid-free paper containing a minimum of 50% recycled, de-inked fiber.

Information contained in this work has been obtained by The McGraw-Hill Companies, Inc. ("McGraw-Hill") from sources believed to be reliable. However, neither McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein and neither McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought

DEDICATION

This book is dedicated to my wife, Karla, for putting up with me during the writing of this book; and to my daughter, Kristen; and son, Jimmy, without whose patience and understanding of late nights and weekends spent writing and rewriting, this book would not have been possible.

ACKNOWLEDGMENT

Thank you Victoria Roberts of Lone Wolf Enterprises for the excellent, expert job you did in editing and guidance; without it this project would not have been possible.

ABOUT THE AUTHOR

Michael Arata has over 15 years of security experience that includes positions from manager to vice president and consultant. He has developed and managed successful security programs from the ground up for several large organizations including the Director of Corporate Security for a major West Coast construction company.

He holds a master's degree in Public Administration, a B.A. in Business/Public Administration, and a B.S. in Safety and Fire Protection Technology. He has attended numerous seminars and training programs relating to security and holds CISSP, CPP, CFE and ACLM, professional certifications.

He has spoken at various professional organization seminars on the subject of security and written articles about security for trade publications. He has guest lectured at the Oklahoma State University and the University of California, Berkeley on safety and security related subjects. He is an adjunct instructor of Criminal Justice at a local college.

Contents

CHAPTER 1 Introduction

The news today is filled with heightened awareness and sensitivity about physical or perimeter security due to the threat of terrorism. What does perimeter security mean? We will explore perimeter security in depth in the book. Perimeter security is defined as the protection of the outer boundary of your facility. With the advent of network security, perimeter security is defined as the protection of outer boundaries of the network. We are only going to focus on physical perimeter security in the book.

What does perimeter security entail? Perimeter security starts at the property line. This is either a natural or manmade barrier. In most cases it is the fence line. Then there are gates, lighting, the building or structure itself, walls, windows, doors, alarms, etc. Sometimes intrusion detection is used to monitor the perimeter fence line or the detectors are located in the ground. In the chapters that follow we are going to explore in detail each of the elements that make up perimeter security.

In Chapter 2 we will examine the security survey and threat assessment. You can't design effective perimeter security that also brings value to the company or the owner without first understanding what you are protecting and who you are protecting it from. Therefore the security survey and threat assessment is the first step. One important aspect is to obtain and understand the crime statistics for the area your project or building is located. The statistics can be obtained from the local police departments. There is also a company that will provide the information and you don't need to purchase any software. All you need to do is to give them an address and they will provide scores for that address based on certain data. The scores are a predictor of the occurrence of crime by type. There are checklists for performing a risk analysis and checklists for completing a security survey.

Chapter 3 will outline the specifications for chain-link fences. The specifications are the Federal DOD requirements which are a standard in the security industry. The types of fences will also be discussed along with their uses. Sample design specifications are also presented.

Chapter 4 is all about protective barriers and how they are effective in physical security and protecting the perimeter. The types of barriers will be presented. The designs and their uses will be discussed. Portable and permanent barriers types and uses are explained.

Chapter 5 addresses protective lighting the types of systems, uses and the design of the protective lighting system to enhance perimeter security. The proper illumination of lighting for security purposes is discussed and the definition of a foot-candle and its importance to security lighting is presented.

Chapter 6 is about access control systems and what is available and the benefits of using dual technology systems. Sample detailed design specifications are provided for the access control system. The integration of alarms and CCTV into one system is discussed.

Chapter 7 presents intrusion detection systems (IDS). The use of dual technology systems when deploying an IDS is discussed. All the types of IDS systems are presented and how they work. Sample design specifications a re included in the chapter for use as a guide for developing a set of specification for a project.

Chapter 8 concentrates on parking garages and parking lots and how to include security into the design and construction of them. The type of lighting that enhances security in parking garages and lots is outlined. The use CCTV and other security devices to help make the users of the parking garage and lots feel safe. As with the other chapters sample design specifications are included in the chapter.

Chapter 9 looks at the world of CCTV. The types of systems used are presented but emphasis is on the digital systems since this is the current trend of the CCTV today. Deign issues are also discussed and as some of the problems that may be encountered in the design and installation.

Chapter 10 is all about locks and keys. The uses of the various locking devices are discussed. Key control programs are also presented. Sample design specifications for deigning locking devices into a project are presented.

Chapter 11 windows and doors are on the perimeter and a likely point of entry for intruders. The ways to protect the windows and doors by using two types of IDS and better locking devices is explored. The chapter has a sample design specification document for designing secure windows and doors.

Chapter 12 the concept of defense-in-depth is explained and how it can improve security in a new facility by designing layers of security. The layered approach will help enhance security because when one layer is defeated there is another layer to tackle for the intruder. The defense-in-depth approach helps to harden the target by making it harder to gain entry and the possibility of being detected.

Chapter 13 secure areas in buildings like storage areas for high value cargo are important to certain types of facility designs. Warehouses that have or will have high value cargo must have a way to protect the cargo to keep the losses to a minimum.

Chapter 14 is the design of perimeter security for new facility for a fictitious company. The company makes vaccines to be used for biological agents and could be the target of various groups so protecting the facility is important to its operation. By designing the security the company can make sure the security meets its security needs and also be part of the architectural design. Also included is a figure showing the security devices on a sample floor plan for the new facility.

Chapter 15 protection of utilities is a sometimes forgotten part of perimeter security since the utilities traverse the perimeter to enter the facility or building. The utilities are the life blood of the facility brining electricity, telephony, and water in. Without the utilities the facility could not operate.

Chapter 16 protecting against explosions either intentional or accidental is important. There are new designs of building structures that can help the building with stand the effects of an explosion. This means that the protection can be designed into a new facility like the walls, structural members, windows and other openings to with stand the effects of explosions and limit the loss of life. Part of the design process is picking a location that can be defended and not be destroyed or severely damaged by being located to a value target.

Chapter 17 outlines fire protection system types including detection. Fire sprinklers and gaseous systems and how they work are presented. Sample design criteria documents for sprinkler systems are included in the chapter. The different types of detection system and how they work are explained. There are also sample design specifications for detection systems provided in the chapter.

Chapter 18 protecting companies from eavesdropping is becoming more of an issue especially if the company works on Homeland Security work like vaccines for biological agents, or new technology for IDS, etc. The types of eavesdropping devices are explained as is the how to design a soundproof room. Other countermeasures that can be added to the design are also discussed.

Chapter 19 shipping and receiving areas are a large vulnerability and need to be designed to help mitigate the possibility of an explosive device being introduced into the facility or building by way of the shipping and receiving dock. In Chapter 20 all the forms and checklists will be in this chapter separated by category.

CHAPTER 2

Threat Assessment and Risk Analysis Basics

Properly designed and implemented perimeter security planning is the key to success. Threat assessment and risk analysis are both important to the process. Perimeter security countermeasures cost money to implement and, to help justify the expenditures, threat assessments and risk analyses are good tools. Threat assessment is the process of determining what the vulnerabilities are and the likelihood that they will result in a loss. To put it simply - what can go wrong resulting in a loss? Risk analysis is taking the vulnerabilities (threats) and determining the likelihood of whether a threat will cause a loss. The purpose of the risk analysis and threat assessment is to make sure the most cost-effective solutions are proposed. So the steps to the process are as follows:

1. Identification of the assets
2. Identification of the threats
3. Analyze the threats (risk assessment)
4. Determine what countermeasure (security feature) will mitigate or minimize the impact of the threat
5. Do a cost analysis so the benefit of the countermeasure selected can be quantified.

Using the survey and the risk analysis, the design specifications for perimeter security of the facility can be developed to meet the threats of the facility. This way the most severe threats and risks are addressed. To identify the threats you need to first identify the assets. Table 2-1 outlines the risk assessment steps and provides a brief description of each one. This is a good summary of the process.

TABLE 2-1 Risk Assessment Steps

STEP	DESCRIPTION
Identification of the assets	People, equipment, buildings, etc.
Identification of the threats	CAP Stats, etc.
Analyze the threats (risk assessment)	Probability of occurrence
Choose countermeasure	Alarms, access control, etc.
Cost analysis of countermeasure	
Cost benefit, ROI	

This chapter is an overview on how to do a threat assessment, including some useful tools to aid in the process such as a cost benefit analysis. To fully understand the concepts in the chapter there are some terms that need to be defined:

1. Threat assessment—What can or will cause harm or loss to the people, facility, and products - vulnerabilities
2. Risk assessment—The evaluation of the threats and determining which ones pose the greatest potential to cause harm. The analysis is used to categorize the threats in rank order by the highest probability of occurrence.
3. Risk management—The process used to minimize the exposure to loss

There are entire books devoted to risk management that include risk assessment, analysis, and mitigation. Formulas are used to determine the probability of a potential loss occurring and what the dollar of the loss would be. For the purposes of our discussion, we will keep it basic. The basics outlined in this chapter are effective tools and are easy to use.

HOW TO DO A THREAT ASSESSMENT

A threat assessment is the first step in determining what perimeter security will be needed. The assessment is the first step in risk analysis and is used to determine the threats and vulnerabilities. Conversely, the first step in risk analysis is identifying the threats. Why do we need do a risk assessment you may be asking? The following will give the reasons why:

1. Security costs and money is limited.
2. Justify the expenditures
3. Be a part of the risk management program

The risk management program has two methods for achieving the goal:

1. Pay for loss prevention countermeasures
2. Purchase insurance

The risk management program has the following steps:

1. Identify the risks
2. Analyze the risks for probability of occurrence
3. Choose the method of mitigating the risk
   a. Risk avoidance
   b. Risk reduction
   c. Risk segregation
   d. Risk acceptance
   e. Risk transfer (purchase insurance)
   f. Combinations of any of the above
4. Continually re-evaluate the steps above

Identify the Risks

Now let's look at how we can identify the risks. The security survey is a tool that can be used to identify the risks. The survey starts by looking at the location of the building or structure. The purpose of the survey is to provide the information necessary to make decisions on what level is security is needed. To effectively perform the survey, you need to collect some background information about the crime statistics in the area of the proposed or existing building or structure. The survey form and the crime statistics are used to determine the threat to the facility, which is the first step in risk analysis. What you are looking for is the type of security features that will best meet the need. So looking at crime statistics is an important first step. The following steps are an abbreviated version of what the security survey is all about:

1. Where is the facility located or where will it be located?
2. Crime statistics for type and frequency?
3. What type of facility or structure will be or is at the location?
4. What is it you are trying to protect?
5. Who are trying to protect it from?

6. What is the best way to protect the facility, people, and process?
   a. External intrusion detection
   b. Access control
   c. Video surveillance (CCTV) monitoring
   d. Locks and keys
   e. Clear zones
   f. Security officers
   g. Controlling vehicular and pedestrian traffic
7. What natural barriers can be used in the protection and design plan?
   a. Rivers
   b. Cliffs
   c. Beaches
   d. Other rugged terrain

The most effective way to collect the information necessary to identify the risks is to have some kind of form or checklist. These forms are extremely helpful and make the job easier by ensuring that all the information is collected and recorded. The forms can be simple to comprehensive. The more comprehensive the form, the more accurate the survey and risk analysis will be.

Analyze the Risk for Probability of Occurrence

So we want to know if an event will happen that will cause a loss. This is also known as the probability of risk occurrence. There are various methods used to determine the probability of risk occurrence. Some are simple, such as the Simple Probability Formula. Others are more complex and will left for the risk management books and books on statistics. For our discussion we will look at the simple formulas.

A simple explanation of probability is given by the action of tossing a coin. The action will generate one of two outcomes, either heads or tails. If the coin used is perfectly symmetrical, the probability would be 1/2 (.5 percent) for heads, 1/2 for tails (.5 percent). The probability measure of an event can be defined as the ratio of the number of outcomes. Therefore, when you toss the coin, the odds are that heads will come up in half of the tosses and tails will come up in the other half of the tosses. Thus if you toss the coin 100 times and you get tails 50 times, then a probability measure of 50/100 to the event that the coin will come up tails on the toss.

$$\text{Simple Probability} = p(\text{Event } 1) + p(\text{Event } 2)$$

The Probability of Event 1 plus the probability of Event 2

Then there is the probability of related events.

$$\text{Probability of Related Events} = \\ p(\text{Event 1}) \times p(\text{Event 2}) = p(\text{Both Events})$$

The Probability of Event 1 times Probability of Event 2 gives the probability of both events occurring.

Let's look at an example of how you can use the simple probability formulas. Event 1 and Event 2 are two independent events and the probability that both events will occur is determined by the product of their separate probabilities. The probability that either of the events will occur is the determined by the sum of their separate probabilities minus the probability that they both will occur. Event 1—there is an unprotected window on the first floor. Event 2—the burglar forces entry through the unprotected window and steals computers with company secrets. So we add the probability of each event together to see the likelihood that the events will cause a loss.

To use the formula we need to assign numbers to the events. The probability Event 1 will happen is 0.5, the probability that Event 2 will happen 0.8. The probability both events will happen is 0.5 × 0.8 = 0.4 and the probability that either Event 1 or Event 2 will happen is 0.5 + 0.7 − 0.4 = 0.8. So there is an 80 percent probability that one Event will occur and a 40 percent that both events will occur.

There are matrices that rate an event for low to high as seen in the tables that follow. Matrix tables that rate probabilities from high to low are used to predict frequency. They are based on past performance and other data such as the CAP crime statistics of an address. A company called the CAP Index provides excellent crime statistics and tables to aid in the decision making by providing information to determine the type and probability of crime occurring at the chosen location. More will be presented about the CAP crime statistics later in the chapter. They are an accepted method of rating risk.

The numbers in Table 2-2 can be used to explain the severity of an event from "Low" to "High". The numbers can take on any number of representations. For example, take our earlier example of the unprotected window and the burglar.

TABLE 2-2 Risk Matrix

	PROBABILITY OF OCCURRENCE		
SEVERITY	HIGH	MEDIUM	LOW
High	1	2	3
Medium	4	5	6
Low	7	8	9

If the crime statistics show from the CAP report that burglaries have a high incidence of occurrence, you would select the probability of occurrence as 1. Now if a burglary does occur, you have determined that the loss would be severe so you give the severity a 1 as well. The result is a "High". "High" in the matrix means the severity is high as is the probability of occurrence. Action should be taken on reducing the exposure by implementing some countermeasures.

Calculating the Cost of a Loss

Now that we have calculated the probability of a risk occurring, we need to go one step further and calculate the cost of the loss so we then calculate whether the cost of avoidance is worth the expense. This is an important step in the process because expenditures for security, like any business expense, need to be justified. This is also known as a Return on Investment (ROI). If the cost of the security countermeasure is greater than the loss, the measure will not be implemented. For example, let's say the cost of the countermeasure will be $20,000 but the potential loss is only $2,000. Then the countermeasure will not be implemented. The process will also aid you in decisionmaking by prioritizing where the dollars will do the most good. To do this we can follow the steps below. (Based on information from http://www.epmbook.com/risk.htm "Risk Management: Who, What, Why", Simon Wallace copyright 2002).

1. Calculate the expected loss. There is a basic equation used to determine the cost of a loss.

   Probability of the Risk × Cost if it happens = expected cost if it happens

2. To justify the avoidance actions the following can be used to calculate the net benefit of the cost avoidance and/or reduction.

   Quantifying Risks and Justifying Avoidance Expenditures

   Probability × Financial Impact = Expectation of Losses

   .8 × $50,000 = $40,000 Expected Loss

   Where .8 is the probability of an event occurring times the $50,000 the financial impact equals the expected loss.

   Below is the amount of the expenditure to prevent or reduce the loss.

   $15,000

   Probability after effect of avoidance and/or reduction actions × Financial Impact after effect of avoidance and/or reduction actions = Revised expectation of losses

   .1 × $50,000 = $5,000