CONSTRUCTION SITE SECURITY

- Recognize and address threats to construction site security
- Ensure worker safety and protect assets and equipment
- Use downloadable checklists, survey forms, and questionnaires for a quick start to a safer site

Michael J. Arata, Jr.

Construction Site 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 0-07-146029-2

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 Overview

Each of the components of security listed below has its own subset. This book will focus on physical security countermeasures and how they can be applied to the construction job site. Security encompasses several components:

- Physical
- Personnel
- Investigations
- Awareness
- Information security

Physical security is the protection of people and things from harm by using such methods as intrusion detection, access control, and security officers. Physical security countermeasures are the measures used to safeguard personnel from harm. It also protects property from unauthorized access to equipment, installations, material, and documents and safeguards it against sabotage, damage, and theft. The main objective of physical security is to harden the target and make it unattractive for thieves and vandals to enter the site for fear of being caught. Target hardening will not deter those individuals who are highly motivated and determined to enter the site to steal or commit vandalism. If the target looks hardened, it will deter most thieves from feeling that there are easy pickings on the site so they will go to a place where there are no security countermeasures. Physical security, in some cases, can be a delaying tactic to slow down an intruder in order to increase the possibility of being seen from outside the perimeter by patrolling security officers and/or police.

Most physical security countermeasures that are used in the private sector have their origins in the government defense and national security programs. Companies that do government contract work, especially defense or any work that is of a national nature, are required by the government to have a security program. There are inspections (audits) of the company's facilities to ensure compliance with the security requirements. Part of the audit is a threat assessment to identify the vulnerabilities. Then, recommendations are made to address the vulnerabilities. The same scenario is used in other private sector companies. The government is not involved unless there is a national security reason, such as with the country's infrastructure including the utility companies, water, electric, and/or rail transportation.

The general public perception is that physical security is guards, guns, and dogs. Nothing can be further from the truth. Physical security is more than the perception since it involves the employees of the company through the security awareness program and policies, as well other countermeasures like intrusion detection. The purpose of this book is to dispel the perception and present the specifics involved in the securing of a construction job site.

Construction job sites present a unique set of issues when addressing physical security. Some of those issues are:

- The site is usually in a state of flux that is it constantly changing.
- The site perimeter is fenced by a temporary fence that will move as the site changes.
- A great deal of traffic entering the site during working hours
- Often, there are no clearly defined roles and duties for the security officers.
- Intrusion detection is hard to position for the perimeter because of the changing environment and the cost.
- Lighting is, at times, not adequate to deter would-be thieves from helping themselves to materials, equipment, and tools.
- Closed Circuit Television (CCTV) systems are usually designed with security in mind.
- They usually show progress of the project on a web cam.
- The cost of security: Who pays?
- Universal keys for starting heavy equipment
- Job site trailers are easy targets for thieves.

In this book we will look at the definition of physical security and how it can be applied to the construction job site. There is no one way to approach implementing physical security countermeasures, but there are some steps that can be taken to help minimize the threats and the vulnerabilities to a job site. To do this there are some concepts that need to be explained. The first one is a threat assessment: what it is; why it is important; and how it helps in physical security planning.

THREAT ASSESSMENTS

Properly designed and implemented physical security planning is the key to success. Threat assessment and risk analysis are both important to the process. Physical 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. Therefore the steps of 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

In Chapter 2, more will be discussed about threat assessments and methods for doing them, including checklists that can be helpful.

The Role of Threat Assessments in Physical Security

The threat assessment plays an important role in physical security by helping identify the most vulnerable areas. The threat assessment will help in planning the physical security countermeasures to minimize the risk from the vulnerabilities. It is the first step in the process of planning for physical security countermeasures and helps determine what to protect against based on the probability of occurrence. The probabilities of threat occurrence are then categorized as low, medium, or high. The high threats are the ones that should have countermeasures in place to minimize the risk. Details of the threat assessment process are explained in Chapter 2.

After the threat assessment is completed and the risks associated with them are identified, a set of recommendations is formulated based on priority established by the probability of risk occurrence. A countermeasure is developed to mitigate the threat and the resulting vulnerability that was discovered in the assessment. These countermeasures become the recommendations. A countermeasure can be one or a combination of the following:

- Intrusion detection systems
- Security officers
- Access control
- Perimeter controls
- CCTV
- Security lighting

Intrusion detection systems can be integrated into the CCTV system so there is a record of who made an unauthorized entry into the job site. Intrusion detection systems can be used in conjunction with the access control system to receive an alarm of an unauthorized entry or attempted entry. This is important for the job site office trailers as well as the tool trailers that may be on site. The intrusion detection system along with access control can also be integrated with the CCTV system to record any events that occur after hours. More about intrusion detection will be presented in Chapter 6.

Perimeter controls, such as access to the site by vehicles through gates, can be controlled by security officers if necessary. Good lighting is also important for physical security because it makes it easy for someone to be seen at night on the site from outside the perimeter.

Threat assessments help managing the risks posed by the security vulnerabilities. After the threat assessment is completed, a set of recommendations (countermeasures) are made based on the risks posed by each threat. The physical security countermeasures are used to offset the vulnerabilities and risks.

Threat assessments help identify the following:

- Who
- What
- When
- Where
- Why
- How

With each vulnerability, the five "Ws" and the "How" questions are asked to determine the extent of the risk of occurrence of the threat. Threat assessments can be an arduous task and may seem to be waste of time and resources. Nothing can be further from the truth. The time it takes to complete a threat assessment is well worth the effort because, by addressing the highest priorities, you get the most from the money you have to spend on security. Threat assessments have a positive impact on physical security spending when properly and conscientiously done. Money is spent judiciously to mitigate the greatest threats that have the highest probability of occurrence. The old 80/20 rule applies here. By taking care of the top 20 percent of the threats, you then will have addressed 80 percent of the security problem. Also the threat assessments will help in focusing on the 20 percent by prioritizing the most likely security events by probability of occurrence.

In some cases the countermeasures will not entirely mitigate the threat, but can substantially reduce the impact from the threat if it does occur. In other words, not every countermeasure can stop a security event by those who have much to gain and who are determined and motivated enough to carry out the threat. For example, if stealing heavy equipment from a job site can be done in 10 minutes or less and someone is willing to purchase the stolen equipment, then the risk of stealing the equipment maybe worth the risk of being caught. Therefore, the job of the countermeasure is to make it appear to the thief that it will take longer than 10 minutes to gain access to the equipment in order to steal it. For example, if the job site is a road construction project, the following countermeasures could be implemented:

- Placing all of the heavy equipment at the end of the work day in a fenced area that can be seen on all four sides from the roadway
- The equipment storage area should have sufficient lighting and a clear zone of five feet around the fence perimeter
- All of the equipment should have some type of kill switch so it cannot be easily started.
- All equipment serial numbers should be recorded and signs should be posted around the site to that effect. It should also be stated that there is a reward for information leading to the recovery of the equipment and the arrest of those responsible for the theft.
- Wireless CCTV can be used along with wireless motion sensors to detect any intrusion into the equipment storage area.

These countermeasures may make the site unattractive to the thief because of the fear of being caught. On other job sites the equipment can be placed in a fenced-in area as close to the center of the site as possible. The thieves would then need to go through two fences that are not close to each other. The first fence would be the perimeter fence and then the thief would need to go through the open well-lighted job site to get to the equipment storage area that is also well lighted. More will be discussed about countermeasures to secure heavy equipment in Chapter 9.

Remember, the objective is to harden the target or at least to create the appearance that the target is hard. The thief may think twice about attempting to steal the heavy equipment. In order to make the target appear hard, set up a perimeter which includes lighting and clear zones.

PHYSICAL SECURITY

Physical security protects people and things. Network or Information Technology (IT) security protects the information that is on computer hardware, software, and email. The physical protection of the computer hardware is a physical security function. The protection of the logic, i.e. software, information is an IT security function.

The countermeasures that will deter, detect, and respond to security incidents are called physical security. Overtly making the site appear hardened can deter security incidents. This includes perimeter controls. Even a temporary fence with locked gates provides some sense of control. Good lighting that lights up the site, CCTV cameras, and roving security patrols are other excellent countermeasures.

The detection of intruders can be done using various techniques like motion sensors. For job site trailers and buildings, door and window contact switches can be used. CCTV can record intruders entering the site. In order to be effective some design considerations need to be taken into account and Chapter 8 will provide the details about CCTV systems.

The response to security incidents is the responsibility of the security officers, if the site has them. If properly trained and provided with a good set of POST orders, the security officers can provide an effective layer of security. POST orders are the procedures that the security officers are supposed to follow during every shift. Chapter 11 will outline the role of the security officers at a job site.

Perimeter security can be enhanced by including the following countermeasures:

- Intrusion detection
- Security officers
- Security lighting
- CCTV
- Warning signs, i.e. "No Trespassing"

The Role of Technology in Physical Security

There have been a number of technological advances in physical security. Some of these advances are in the intrusion detection systems. One measure is the ability to integrate the access control systems into the CCTV system. By having all the systems integrated together, they are more efficient and the security officer need only look at one screen instead of several screens for alarms and access control information. CCTV cameras and controls for pan, tilt, zoom (PTZ) cameras are very useful in this case. Wireless cameras and instruction detection systems are now available and being used.

CCTV cameras can record on DVD instead of VHS, so there is no need to change tapes. This solves the problem of not getting the recording of a security event because the tape was either full or no tape was in the recorder. The CCTV cameras today can be set to record on motion and will record in real time instead of time lapse.

Technology plays an important role in physical security now and will do so in the future. Technology can improve the efficiency of the security officers by increasing their productivity.

SUMMARY OF THE CHAPTERS

The purpose of this book is to outline some methods and techniques for security construction job sites. The techniques outlined in the book are not the only way to approach the security issues facing construction sites, but offer some good basic security concepts and methods that can be employed to help protect the site. The book has five parts and the chapters associated with each are outlined below.

Part I is "Understanding Security" and outlines what physical security is all about and why it is important.

Chapter 1 is an introduction to some of the concepts and ideas that are presented throughout the book. Definitions of what the concepts mean are presented, especially the threat assessments and their importance.

Chapter 2 presents a detailed discussion of threat assessments, their importance, and how to do them. There are checklists to help guide you through the process. The benefits of performing the threat assessment are presented.

Chapter 3 is an overview of security and everything that is covered in the book is summarized for quick reference. Details about each of the subjects covered in the chapter are explained in detail in other chapters.

In Chapter 4 the security survey is discussed in detail: what a security survey is; the benefit of doing them; and how to do them. There are sample checklists and forms for doing security surveys in the chapter.

Part II is all about "Physical Security," what it is, what are the countermeasures used, and how to implement them.

Chapter 5 outlines what can be done to establish perimeter security. A perimeter fence, even a temporary fence, will help in establishing a perimeter security boundary. Incorporating and using any natural boundaries in the perimeter security plan is mentioned. Rivers and cliffs, to name two, can be assets if they are assimilated into the perimeter security. Clear zones around the perimeter fence and other fenced areas on the job site are discussed and why they are an important buffer.

Security lighting for the perimeter is also discussed in the chapter, since this an area that is often overlooked on construction job sites and can be a benefit.

There is a section in the chapter about establishing control points, namely the entrances to the site during business hours and after hours. Controlling access to the job site is important in order for unauthorized persons or vehicles to have difficulty entering easily.

Chapter 6 explores the types of intrusion detection systems. The technology of the systems is explained, as are the applications for each type of system. Also discussed are the problems with each of the intrusion detection systems, i.e. the causes of false alarms.

Chapter 7 discusses locks and key control. This has been and continues to be a difficult problem, but there are technological advancements to help manage the key control system. The types of locks useful for a job site will be presented.

Chapter 8 is all about CCTV systems. The types of systems are presented as are some basic design requirements for an effective system. Why security lighting is important to an effective CCTV system is also discussed.

Chapter 9 takes a look at ways to secure the equipment on a job site. There are some basic things that can be done, such as having a complete record of all serial numbers for all equipment assigned to the job site. The use of kill switches is discussed as a strategy for deterring thefts of heavy equipment from the site.

Chapter 10 discusses access control. Access control technologies have come a long way in the last several years. The systems are more user-friendly for the system administrators and there is research work being done in the use of wireless readers. Access control keeps unauthorized persons offsite and accounts for those who are on site, especially in the job site trailers. Since there is a great deal of vehicle and pedestrian traffic at some job sites, some type of control, especially the control of trucks and private cars, will be helpful.

Chapter 11 explains the role of the security officer. Security officers can be a valuable asset in physical security by helping control vehicle traffic and the flow of pedestrians through access points. Security officers can also provide a good deterrent to vandalism and other types of crimes to the property and equipment by performing patrols around the perimeter after hours at unscheduled intervals. In