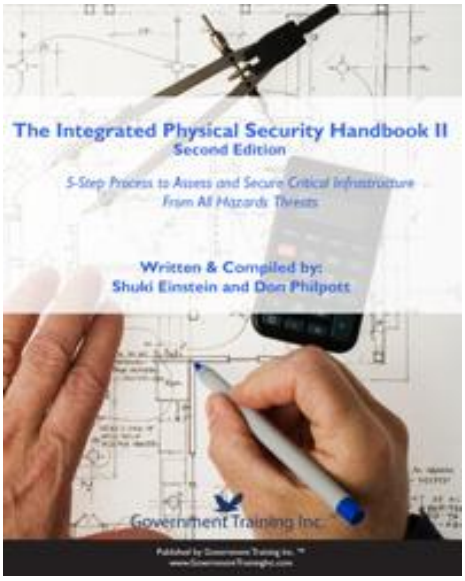
Government Training Inc.™

This PDF file contains the following excerpts from the book:

- Table of Contents
- About the Authors
- Forward and Introduction



The Integrated Physical Security Handbook II

Second Edition

5-Step Process to Assess and Secure Critical Infrastructure
From All Hazards Threats

Written & Compiled by:
Shuki Einstein and Don Philpott

ISBN: 978-0-9832361-0-8

Published by:
Government Training Inc

About the Publisher – Government Training Inc. ™

Government Training Inc. provides worldwide training, publishing and consulting to government agencies and contractors that support government in areas of business and financial management, acquisition and contracting, physical and cyber security, intelligence operations and grant writing. Our management team and instructors are seasoned executives with demonstrated experience in areas of Federal, State, Local and DoD needs and mandates.

Recent books published by Government Training Inc. ™ include:

- The COTR Handbook
- Performance Based Contracting Handbook
- Managing Cost Reimbursable Contracts
- Guide to Independent Government Cost Estimates
- The Grant Writer's Handbook
- Handbook for Managing Teleworkers

- Handbook for Managing Teleworkers: Toolkit
- Small Business Guide to Government Contracting
- Workplace Violence
- Securing Our Schools
- The Integrated Physical Security Handbook (First Edition)

For more information on the company, its publications and professional training, go to www.GovernmentTrainingInc.com.

Printed in the United States of America.

Government Training Inc. ™
Rights and Contracts Department
5372 Sandhamn Place
Longboat Key, Florida 34228
don.dickson@GovernmentTrainingInc.com

About the authors

Don Philpott

Don Philpott serves as Publishing Editor for Government Training Inc. and has been writing, reporting and broadcasting on international events, trouble spots and major news stories for more than 40 years.

For 20 years he was a senior correspondent with Press Association -Reuters, the wire service, and traveled the world on assignments including Northern Ireland, Lebanon, Israel, South Africa and Asia.

He writes for magazines and newspapers in the United States and Europe and is a regularly contributor to radio and television programs on security and other issues. He is the author of more than 90 books He has written special reports on Protecting the Athens Olympics, The Threat from Dirty Bombs, Anti-Terrorism Measures in the UK, Nanotechnology and the U.S, Military and The Global Impact of the London Bombing. Security books published by

Government Training Inc and authored by Don Philpott include: Securing Our Schools, Workplace Violence and Integrated Physical Security Handbook – 1st Edition.

Shuki Einstein

Shuki Einstein is an architect and an internationally recognized security expert and strategic planner. Born in New York he moved to Jerusalem at the age of 9. He served in the Israel Defense Force, trained as an architect at the Technion – Israel Institute of Technology in Haifa and practiced as an architect in Israel for 14 years. He was the CH2M Hill Architectural Discipline Coordinator in the Middle East office before relocating with his family to Portland, Ore., in 2000.

His design experience has included numerous complex projects involving integrated multidisciplinary coordination, from front-end conceptual design to development of construction documentation. In addition to traditional architectural design, his experience also includes master planning, interior design, and project management, and he has managed projects in Europe, the Middle East, Asia and North America.

He has extensive experience in integrating architectural physical protection systems with functionality, maintenance, operations and access control systems. He is a nationally recognized counterterrorism expert, consultant, and speaker, and his areas of expertise include vulnerability assessments, security master planning and security awareness training.

Einstein currently lives in Portland, Ore., with his wife and three children. He is an executive board member for Architects Without Borders – Oregon

Table of Contents

Forward

Our nation and the world have changed dramatically since the tragic events of September 11. It is not just our facilities and institutions that are threatened; our freedoms and the quality of life that we hold so dear are also under attack.

We have the dual responsibility of ensuring that the facilities and buildings where we work and play are as secure as possible and at the same time, we have to maintain an acceptable quality of life.

Integrated physical security planning does not mean reverting to a bunker philosophy. It does, however, involve a sometimes difficult balancing act between effective and adequate security and being able to carry on business as usual.

Measures that have been and continue to be taken to protect and defend our homeland have made us all safer but we still live in troubled times.

Today's terrorists can strike at any place and at any time and with a wide variety of weapons.
Our critical infrastructures, like ports, power stations and water treatment plants, are an obvious target but so are millions of other facilities nationwide where tens of millions of Americans work every day.

There are also countless threats that we face, both natural and man-made – from hurricanes, floods and earthquakes to theft, workplace violence and serious crime - that need to be addressed.

Vulnerable facilities include local, state and federal government buildings and private offices, as well as schools, hospitals, places of worship, food outlets, malls, theaters and sports arenas.

While most of us take steps to protect our homes and our personal possessions, many facilities both public and private, do not receive the same security protection putting the buildings and assets – including the people who work and visit there - at risk.

Many facility managers have taken the view “It won’t happen to me” - but it might. Even if your building is not a target, have you considered the consequences of an explosion at a nearby facility and how that would impact on your business and people?

That is why integrated physical security planning is so critical. Once you have identified the threats and vulnerabilities, you can prioritize the assets that need to be protected. You are then in a position to develop a physical security plan to defend them.

A secure facility is a safer facility and by working with local government, neighboring properties, law enforcement and fire, you can help in building safer and more secure communities.

The challenge is enormous but steadily we will prevail. The more facilities and buildings that implement integrated physical security systems, the safer we all become. This helps protect us against terrorism and disasters and make us safer and more secure. It is how we can all help build a better and stronger America – one facility at a time.

John A. Gordon, General
U.S. Air Force (Retired)
Formerly President’s Homeland Security Advisor

The Integrated Physical Security Handbook

Second Edition Highlights

This new edition covers a number of additional areas including convergence of systems, building modeling, emergency procedures, privacy issues, cloud computing, shelters and safe areas and disaster planning. There is also a comprehensive glossary as well as access to a dedicated website at www.physicalsecurityhandbook.com that provides purchasers of the book an on-line library of over 300 pages of additional reference materials.

The first edition was bought by corporations and government agencies worldwide and ASIS International in its five-star review said, "This is an excellent textbook for novice security managers and a great desk reference for industry veterans."

This new, expanded and updated edition makes it an even more invaluable resource.

Introduction

Protecting America One Facility at a Time

Overview

More than half the facilities in the United States do not have a crisis management plan – what to do in the event of an emergency - and many that do, do not keep it up to date. Even fewer businesses and organizations have integrated physical security plans to protect the facility and people who work in it.

While alarming, this statistic is not surprising. Until 9/11 most businesses and facilities took the attitude: "it will never happen to me'. On 9/12, tens of thousands of managers across the country were called in by their bosses and told they were now responsible for facility security – some knew what was expected of them, others did not. Ten years on, that is still a major problem and that is what this handbook sets out to address.

The catastrophic effects of Hurricane Katrina and the subsequent flooding, the earthquake in Haiti and the devastating oil spill in the Gulf of Mexico are all somber reminders of just how critical good planning and preparedness is. The biggest mistake made by emergency managers planning for a Hurricane Katrina-type event in the Gulf States was that they made assumptions. They assumed the coastline would not get hit by anything above a Category 3 hurricane and they assumed the levees protecting New Orleans would hold. Both assumptions proved to be deadly errors. Never assume anything and especially never assume that it can't happen to you.

The process of developing an Integrated Physical Security plan demands that you consider all conceivable threats, even the doomsday ones, so that you can come up with effective plans to mitigate them. That is the only way to protect our nation's facilities and the people who work in them.

The Challenge

The challenge is twofold. The first challenge is to get agreement that something needs to be done. This involves altering mindsets; building consensus and getting senior management buy in. The second challenge is in developing and implementing an effective and tailor-made integrated physical security (IPS) plan. This plan consists of three mutually supporting elements –

- Physical security measures
- Operational procedures
- Policies.

Physical security covers all the devices, technologies and specialist materials for perimeter, external and internal protection. This covers everything from sensors and closed circuit television to barriers, lighting and access controls.

Operational procedures are the lifeblood of any organization - they cover how the facility works on a day to day business, shift changes, deliveries, when maintenance is carried out and so on. You must understand how the facility works and operates in order to develop an effective integrated physical security plan that allows it to get on with its job with the least disruption as possible.

Equally you must recognize that any effective IPS is going to impact on operations – things will change and you have to both manage and plan for change and ensure that the reasons for the changes are understood and accepted by all personnel.

Policies spell out who does what and the actions to be taken to prevent an attack or incident, or should one take place to mitigate its impact and ensure continuation of business.
This handbook is designed to walk you through a five steps process. It will tell you what needs to be done and why and then tell you how to do it.

The Five Step Process
Step 1: Your Model Secure Facility
Step 2: Gap Analysis
Step 3: Gap Closure
Step 4: Strategic Plan
Step 5: Implementation

Ultimately almost any IPS is a compromise because you can't make a facility 100% secure if you have a continual flow of people and vehicles coming in and out. The aim, however, must be to develop an integrated physical security program that meets all key objectives and provides the maximum protection against defined threats with the resources available.

The other major consideration is in knowing when enough is enough. It is possible to keep adding enhancements and new security levels but again, there has to be a compromise. At what point does there cease to be a quantifiable benefit in spending more money, especially if the security levels become so stringent that they impact your ability to conduct business as usual.

The goal of implementing an integrated physical security plan is in achieving sensible security, sustainable security.

A secure facility is a safer facility and by achieving this you boost morale and wellbeing.

The goal of this handbook is in making all our facilities and buildings secure and safe while maintaining in our offices and workplaces the quality of life that we have come to expect over many years. Our target is making America safer – one facility at a time.

This Five Step Process enables you to understand the different elements that need to be considered when developing your integrated physical security plan. Essential to these elements are who and what we are protecting:

- People – the people that work in and visit the facility, those working and living nearby and those who rely on your products and services.
- Operations – the day to day running of the facility covering everything from shifts and deliveries to maintenance and utilities.
- Information – information/data sources and protection, communications internally and externally.
- Assets – other than people cover anything that is key to your mission that can be destroyed, damaged or stolen, and
- Inter-dependence – how what happens at your facility may impact on the wider community and how incidents at neighboring facilities might impact on you. You have to be aware of what us happening upstream and downstream of your facility.

When developing a plan each of these categories has to be protected and the relationship between each has to be taken into account. As a result, a model security facility is one where all necessary systems are in place, tried and tested, to protect people, operations, inter-dependence and information without impacting on day to day operations. It is one where everyone knows why the systems are in place and what they have to do. It is a facility where confidence levels are high and people feel safe and secure.

Striking the Right Balance

As you go through this manual you will notice a lot of different levels of detail. It is your choice how deep you want to go and that will depend on a number of factors. These include how

much you already know, the threat level to your facility, the complexity of the facility i.e. does it have multiple tiers of security, and your access to advice from in-house or external experts.

The key challenge in implementing IPS is to do the maximum necessary to ensure the safety and security of the facility and the critical assets within, without impacting on the day to day operational procedures. There is no benefit in implementing draconian security measures if they are so restrictive that the facility cannot function normally or if the people they are supposed to protect feel threatened by them. Equally there is little point in introducing hugely expensive security measures if a) the cost's can't be justified, b) the measures are not justified, or both.

A good example of NOT striking the right balance is the facility manager who goes out and buys a number of security cameras, which he has installed around the building. While the presence of highly visible cameras might increase safety levels, they are not completely effective unless someone is monitoring them – and this had not been taken into account. Who was going to monitor the cameras, how were these people going to be trained, where was the monitoring station to be located, how many monitors would it have, what protocols were in place to initiate a security response etc. etc? Having hired and trained monitoring staff did the overall cost justify installation of the cameras in the first place or would a security guard walking round the facility every couple of hours have been as effective?

Integrated physical security plans are by their very nature a compromise – a careful balancing act between what needs to be done and what can be done weighed against what is in the best interest of the facility and its normal day to day procedures.

Communications

Integrated physical security planning should not be undertaken in isolation. While you are developing the most effective plan for your facility, investigate what similar facilities have done or are doing, speak with security experts and first responders to get their input. Discuss your plans with your insurance company – after all, they have a vested interest in reducing their liability so they may be willing to reduce your premiums if you implement security measures and in some cases, they might even be willing to contribute towards the cost.

It is this communication between facilities and external stakeholders that will enable everyone to share information and help develop best practices nationwide. And, with these communication paths open you will be better able to protect your facility and thus help protect our nation – one building at a time. However, this does raise a paradox – you have to have open communications to ensure stakeholders know what is happening, yet you also have to ensure security so that details about what you are doing does not fall into the wrong hands.

Terrorism is not a new challenge and it is not going to go away any time soon as the events in recent years in Times Square, New York, London, Madrid and Mumbai so graphically illustrated.

So we have a duty to ensure that the places where we work, learn and play are secure and that the people using them are safe.

Integrated physical security planning is also important because risks come from both natural disasters such as earthquakes, floods and hurricanes as well as man-made threats ranging from theft to terrorism.

Vulnerable facilities are buildings that have a gap between their mission and their identified risks. These include many critical infrastructures such as power plants, water treatment works and food processing plants. They also include local, state and federal government buildings and private offices where we work, the schools where our children are taught, the hospitals where we are treated, the churches where we worship, the restaurants where we eat and the malls where we shop.

Many of the facilities most at risk are in urban settings because they do not have enough property to establish robust perimeters – i.e. set back far enough from the road to prevent or mitigate the effects of a car bomb.

It is the process and steps needed to provide integrated physical protection of these facilities that is the focus of this book.