The Integrated Physical Security Handbook

By: Don Philpott & Shuki Einstein

CONTENTS

The Integrated Physical Security Handbook

Introduction

Protecting America One Facility at a Time

Overview

More than half the businesses 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 the people who work in it. While alarming, this statistic is not surprising. Until 9/11 most businesses and facilities had the attitude: "It will never happen to me." On September 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. That problem still exists and this handbook sets out to address it.

The catastrophic effects of Hurricane Katrina and the subsequent flooding are a somber reminder 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 assumed the levees protecting New Orleans would hold. Both assumptions proved to be deadly errors. 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 two fold. The first challenge is to reach an 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 and 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 day-to-day business, such as shift changes, deliveries, maintenance schedules 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 affect 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-step process. It will tell you what needs to be done and why and then tell you how to do it.
Ultimately, almost any IPS is a compromise because you can't make a facility 100 percent 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 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 affect your ability to conduct business as usual.

The goal of implementing an integrated physical security plan is in achieving sensible and sustainable security. A secure facility is a safer facility, and by achieving this you boost morale and well-being.

The goal of this handbook is to make all of 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, and internal and external communications.
- Inter-dependence – how what happens at your facility might affect the wider community and how incidents at neighboring facilities might affect you. You must be aware of what is 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 affecting 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 (for example, 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 interfering with 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 can't be justified, b) the measures are not justified, or both.

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 and 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 toward the cost.

It is this communication between facilities and external stakeholders that will enable everyone to share information and help develop best practices nationwide. With these communication paths open you will be better able to protect your facility and thus help protect America – one building at a time. However, this does raise a paradox – you must 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 do 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 tragic events in London last July 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. These 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 the real estate necessary to establish robust perimeters.

It is the integrated physical protection of these facilities that this handbook focuses on.

Why You Need It
Integrated physical security is a must. Apart from the legal and liability issues, it just makes sense to protect the facilities and people on whom you depend – to keep your enterprise safe and secure so that you can, hopefully, prevent an attack or, if one does happen, survive it.

For many organizations there are added benefits from implementing IPS. During the risk and threat assessment phases of developing an IPS, you frequently discover areas of vulnerability that can be remedied and practices that can be improved. This can lead to improved productivity and efficiency and has an ongoing impact on your bottom line. So by implementing an IPS, you might also increase efficiency and profitability.

The biggest benefit, however, is in increased safety for everyone using that facility. It is essential to effectively communicate the need for IPS to all those concerned and to get them actively involved in the process. After all, one of the cheapest forms of physical security – and among the most effective – is the eyes and ears of the people using the facility.

If people understand the need for vigilance and report anything suspicious, they will all feel safer and more secure. And people need to feel safe and secure.

We will "hit hard the American economy at its heart and its core." – Osama bin Laden

The terrorist threat does not only come from overseas. According to the FBI, there are more than 1,000 pipe bomb incidents every year. In the last eight years more than 40 students, teachers and custodians have been shot dead at incidents in schools. The threat is real and growing.

The Five-Step Process
This Five-Step Process is based on the IPS methodology developed by Denver-based CH2M Hill, one of the world's leading integrated security design companies. The handbook walks you through the five steps needed to identify critical assets, identify threats and targets and take the appropriate mitigating measures to implement an effective integrated physical security system that addresses your specific needs and requirements.

It must be stressed that this handbook addresses integrated physical security. Physical security is the protection of buildings and all their assets, including people.

Integrated physical security recognizes that optimum protection comes from three mutually supporting elements: physical security measures, operational procedures and procedural security measures. That is what this five-step methodology is based on.

In some cases costly physical security measures can be avoided by simple changes to operational procedures. In other instances, the implementation of physical security measures can greatly increase operating efficiency with significant bottom line benefits.

The Five-Step Process

Introduction
In order to carry out a comprehensive assessment of what your facility needs, you have to understand the basic elements of security – what it is you are protecting and how vulnerable it is. You have to know where any threats might come from and what you can do to prevent them or mitigate them. You have to understand the principles of deterrence, detection, delay, response, recovery and re-evaluation. You need to be aware of all the options available to you. Armed with this knowledge you can develop and implement the most appropriate integrated physical security plan for your facility.

When planning, there are two scenarios: if and when. The "if" scenario covers planning and procedures to prevent the likelihood of an incident. The "when" scenario covers planning and procedures after an incident and is mainly concerned with mitigation and recovery.

Remember that the cost to mitigate and recover may be less than the cost to protect, so there always has to be a balance between protection and mitigation.

In effect, IPS is a series of countermeasures to prevent or reduce the impact of an attack. And, as mentioned before, IPS has to be balanced against cost and any disadvantages. Extreme security countermeasures should not be implemented if they disrupt operations or adversely affect the safety of the occupants of a building. For instance, an access controlled door might slow down the evacuation of a building in the event of an emergency.

That is why when designing IPS you first determine objectives and create a plan and then you assess and analyze the design again before implementing it. The plan should contain the following crucial elements –

DDDRRR – deterrence, detection, delay, response, recovery and re-evaluation. These are discussed in greater detail in Security 101, if you need to refer to this, and they are an integral part of your PSS.

- **Deterrence** provides countermeasures such as policies, procedures, and technical devices and controls to defend against attacks on the assets being protected.
- **Detection** monitors for potential breakdowns in protective mechanisms that could result in security breaches.
- **Delay** is a necessary measure if there is a breach, to slow down the intruders long enough to allow a security team to apprehend them before they achieve their objective.
- **Response**, which requires human involvement, covers procedures and actions for assessing the situation and responding to a breach. Note: Because absolute protection is impossible to achieve, a security program that does not also incorporate detection, delay and response is incomplete. To be effective, all three concepts must be elements of a cycle that work together continuously.
- **Recovery** is your plan to continue business and operations as normally as possible following an incident.
- **Re-evaluation** is critical. You must constantly keep your PSS under review and keep re-visiting your original assessment and objectives. Has the situation changed, do you now face new threats and what must be done to ensure the PSS continues to meet your goals and objectives?

Each of these elements has to be planned in relationship to all the others. There is no point in spending money on expensive perimeter fences if there is no detection system in place to warn of intrusion. There is no point in installing sophisticated detection systems if there is nobody around to respond to a triggered alarm. And there is little point in having deterrence and detection without delay if an intruder can gain access, cause damage and get away because there were no delaying measures in place or response times were too slow.

You must understand what you are protecting and from whom. You should never go out and spend money on hardware until you are certain that you are going to achieve the objectives that you have set out.

Step One – Your Model Secure Facility

Now that you have an understanding of basic security techniques and applications relating to facility protection, we next look at a model secure facility – the facility that in a perfect world, is able to able to maximize security without compromising business as usual. Many methodologies omit this and go straight on to the different assessment processes taken as you develop a strategic plan to implement an integrated physical security system. However, we believe it is important that you examine what would constitute a model secure facility for you. This is one which has identified its core functions, identified its critical assets, identified the threats and vulnerabilities and taken the appropriate measures to mitigate them. Above all, it is a facility that is secure, yet one that is able to carry on its core function as efficiently and effectively as before the IPS was implemented. When you come up with your model facility, you have a benchmark for comparison.

Step Two – Gap Analysis: How Do You Compare With the Model Facility?

The goal of physical security is to protect facilities and buildings and the assets they contain. The most important of these assets are, of course, the people who work in and visit the facility. The first things you need to find out are:

• The assets to be protected
• The threat to those assets
• The vulnerability of those assets
• Your priorities

Fact: Eight-five percent of all critical infrastructures and key resources in the United States are privately owned.

What Am I Protecting?
Protective systems should always be developed for specific assets. You have to know the core functions of your facility because that will enable you to identify the specific critical infrastructure that you need to protect to continue in business in the event of an attack.

The goal of security is to protect facilities and buildings and the assets contained inside. Various layers of security may be necessary in different parts of the building depending on the assets located there. For instance, there should be relatively free access to the office kitchen but restricted access to the computer network control room.

Asset value is determined by considering the following three elements:
• The criticality of the asset for its user and/or others
• How easily the asset can be replaced
• Some measure of the asset's relative value

Assets are anything that can be destroyed, damaged or stolen. The risk-analysis procedure is used to identify assets – everything from the building itself to hazardous materials, equipment, supplies, furniture, computers and, of course, people.

Who Are My Adversaries?
It is important to identify and characterize the threat to these assets. This threat can come from within or outside the building. Internal threats include pilfering of office equipment or theft of classified information. Internal threats also include disgruntled employees who may sabotage equipment or attack other employees. External threats range from vandalism and break-ins to acts of terrorism. You need to know your adversaries and the various tactics they might use. You also need to know their motivations and capabilities. Consult with your local police, the FBI and other agencies that monitor these threats. They can advice on what threats you face, from whom and what methods and weapons they might use against them. Two other tools you can use are:

- **Design Base Threat (DBT)** analysis to help identify your likely adversaries, their strengths and capabilities, what their targets might be and the likelihood of them attacking you and, if so, how.
- **Crime Prevention Through Environmental Design (CPTED)** to take into account the relationship between the physical environment and the users of that environment. It is one of the tried and trusted methodologies available to you and is a useful tool in identifying the "bad boys" and what crimes may affect your facility and personnel.

Where Am I Vulnerable?
Until you discover your areas of vulnerability, you cannot develop the strategies needed to protect them. A useful way of identifying threats is to conduct **scenario-based assessments.** This is very analytical process because you must be able to identify all critical flaws and weak points in your current physical protection. You have to come up with multiple "what if" scenarios and work them through. By working through the various scenarios and determining the probable actions and consequences, you can then develop plans to counter or mitigate them.

Use the model facility as your benchmark to identify the areas that need attention. Conduct an audit of the facility – site boundaries, building construction, room locations, access points, operating conditions (working hours, off-hours and so on), existing physical protection features, safety considerations and the types and numbers of employees and visitors.

Next, determine all critical assets – tangible and intangible, equipment, personnel and materials. This analysis should also include reputation, morale and proprietary information.

You must identify and characterize vulnerabilities – weaknesses – that would allow identified threats to be realized. A major problem for buildings in urban areas is the lack of a secure perimeter. In many situations a vehicle containing a bomb could park within feet of a building and cause major damage on detonation. Internal vulnerabilities include poorly trained security staff and lack of access controls to sensitive parts of the building.

Also, assess how you might be impacted by an incident at a nearby facility, such as a chemical spill, and what steps you would need to take to protect your property and people.

By identifying your weaknesses you are able to develop solutions to eliminate them.

What Are My Priorities?
Risk assessment must take into account the effect on your business or operation if assets are destroyed or damaged. Part of that assessment is to rate the impact of the loss of those assets on a scale of low, medium or high. This will identify the critical assets that need maximum protection.

How Do I Compare?
Once you have established the above, you are in a position to do your Gap Analysis to identify what needs to be done to reduce risk, increase safety and provide the necessary physical security for your building and people. How do you compare to the model facility, what are your threats and vulnerabilities? And, having identified these threats and vulnerabilities, how do you prioritize them? Which are the most critical and must be tackled first?

Step Three – Gap Closure
Having identified your shortfalls, you must then consider and evaluate all available options to mitigate the threats. There is a vast array of external and internal systems and devices available. You must determine which are the best options and combinations for your particular circumstances. If you have questions, consult an independent security consultant rather than a vendor with a vested interest in selling you its product.

The options are described in general terms in Step Three and in more detail in Security 101.
1) Perimeter Security
Secure perimeter, perimeter surveillance, protection basics, defense measures, stand-off distances and counter-measures to reduce security risks.
2) Vehicles
Protect approaches, control access and parking, install barriers, surveillance and other monitoring equipment.
3) Internal Security
Access controls, alarms and barriers, authentification devices and screening, access biometrics, closed-circuit television (CCTV), hot site protection, safe mail rooms, coping with hazards.
4) Information Technology
Integrate IT and physical security planning, provide network/infrastructure protection and protect files, document and other critical resources.
5) People
a) Security staff – needs/hiring/training, security programs and responses.
b) Staff/visitors – screening/training/informing; drills/evacuation/safe rooms; alarms/staging areas; communications, and coping with and recovering from an event.
c) Special needs – Americans with Disabilities Act requirements and special resources.

6) Building Design/Security
Building Code laws; exits/fences/gates/doors/barriers/windows; critical floor space/safe rooms/safe areas; devices/detectors; lighting; cameras; and maintenance.
7) Community Risk Assessment/Community Involvement
Assess local risks and incorporate into planning; work with fire/police/EMS; work with local businesses and the community.
8) Technology Solutions
The handbook deals with the various security and defense devices available to you. These are referred to in Security 101 and the Gap Analysis and Gap Closure chapters, but not in as much technical detail as you may wish. References are provided throughout the book to allow you to get more comprehensive information should you need it.

Step Four – Strategic Plan
Having identified assets, adversaries, threats, vulnerabilities and determined priorities and options, you are in a position to plan and strategize the security change process. This means developing a road map – you know where you are and have to plot how you are going to get where you need to be.

The strategic plan sets out Steps Two and Three above – documenting your gap analysis, identifying critical assets, threats and weaknesses and all areas needing to be addressed. The gap closure documents how you plan to close those gaps, the justification for the actions to be taken, costs involved and timeframe for implementation.

The strategic plan serves two critical functions: It is the marketing tool you need to get management approval and it is the blueprint for your physical security plan.

Step Five – Implementation
Once your strategic plan has been approved, it must be implemented. This includes project management, bid contracting and vendor selection, quality assurance and quality control, and revising policy procedures.

Integrated physical security planning is also an ongoing requirement. Once your system is in place you must continuously test it for weaknesses and vulnerabilities. You must ensure your employees understand the measures in place and what they must do in the event of an emergency.

Re-analyze your current situation. Ask yourself what has changed and what new threats have emerged. By constantly tracking and monitoring your integrated physical security system you can close any gaps and introduce enhancements.

Taken together, these five steps will allow you to understand the methodology needed to design and implement effective IPS and then maintain it to ensure that your building, its assets and its people remain safe and secure.

Summary

The Integrated Physical Security Handbook is the essential handbook for facility security managers and all managers and supervisors tasked with the security and safety of the buildings in which they operate and the people with whom they work. It sets out how to manage change and how to conduct crucial threat and risk assessments, the basis for all integrated physical security planning.

Then, using checklists and standard practices, it provides a hands-on, how-to guide that leads you in a user-friendly way through all the steps and processes needed to evaluate, design and implement an effective integrated physical security system.

The handbook is a preparedness tool that could help protect lives and ensure the continuation of businesses, institutions and critical infrastructures in the event of a terrorist attack or other major emergency. As a result, it is a handbook that you cannot afford to be without.

#####
(sidebar)
The Current Situation – How Secure Are You?
There are:

- More than 1,800 government-owned buildings and more than 6,200 leased locations throughout the 50 states and Washington, D.C., employing almost a million federal workers and hosting tens of millions of visitors.
- 327,000 education buildings in the 50 states and D.C. There are 87,630 schools with 47 million children enrolled and employing approximately 3 million teachers.
- 7,569 hospitals nationwide employing 2.4 million registered nurses, 1.8 million nursing aides, 819,000 physicians and surgeons, 350,000 therapists. On any given day there are 539,000 hospital inpatients plus visitors.
- 127,000 additional healthcare facilities nationwide offering inpatient/outpatient treatment.
- 133,000 malls and strip malls and 534,000 large stores nationwide.
- 1 million plus office buildings nationwide.
- 305,000 public assembly buildings nationwide.
- 307,000 churches nationwide.
- 603,000 warehouses and storage facilities nationwide.
- 349,000 food service facilities nationwide.
- 153,000 hotels and motels nationwide.

How many of these buildings and facilities have an effective physical security system in place? How secure is your facility?

#####

The Five Steps

Step One – The Model Facility

Overview

The model secure facility is one where all critical assets have been identified, the threats to them identified and prioritized and effective security measures put in place to mitigate them. All this has been done in consultation with all outside stakeholders, including first responders, and in compliance with local, state and federal mandated requirements and all appropriate regulatory drivers. Above all, the physical security plan has been implemented with management and employee buy-in, to budget and on time with minimum ongoing disruption to the facility's day-to-day operating procedures.

Of course, this is the ideal situation, but let us assume that you have been tasked with designing and implementing the perfect physical security plan. These are the steps you need to take.

Planning

Your aim in developing a model facility is to give you a benchmark to work with. By working your way through the Assessment Checklist and implementing the very best solution to each line item (where appropriate) you should finish up with the model integrated protection system for your facility. You can then compare your current situation with your model facility – the Gap Analysis – and see what needs be done to correct the situation.

Your purpose at this stage, however, is to develop the model facility and not to focus on the gaps which are dealt with in Step Two of our methodology.

First you must set up your core team. This should include you as the project manager, the security and IT managers and all those who have responsibility for operational, building, system and maintenance functions in the facility.

Together, the project team coordinates the preparation of the assessment schedule, assessment agenda and on-site visit assessments with the building stakeholders. It is important to emphasize that the team includes professionals capable of evaluating different parts of the buildings and familiar with engineering, architecture and site planning. Other members of the team should include security consultants, law-enforcement agents, first responders, building owners and managers, and a representative from the facility's insurers.

From day one, the team must involve senior management so that they are aware of what is going on and the changes that will be coming so they can plan accordingly.

Throughout this process you must ensure:

- Confidentiality – the need to protect critical planning documents
- Appropriate Public Relations – keeping the right people in the know while ensuring that information did not get into the wrong hands
- Sustainability – incorporating existing systems into the plan rather than replacing, implementing baseline security where appropriate, balancing physical protection systems with operational procedures
- Compliance with all industrial guidelines and legal and regulatory requirements
- Constant review and revision to accommodate new circumstances or threats

The Model Facility

Remember that the aim in developing your model facility is to identify all critical assets – tangible and intangible – and reduce the risks to them to an acceptable level. You must take into account the following crucial elements – deterrence, detection, delay and response and then recovery and re-assessment. All are mitigation measures. These are the foundations on which any integrated physical security plan must be built.

- **Deterrence** – provides countermeasures such as policies, procedures, and technical devices and controls to defend against attacks on the assets being protected.
- **Detection** – monitors for potential breakdowns in protective mechanisms that could result in security breaches.
- **Delay –** provides measures that in the event of a breach delay intruders long enough to allow a security team to apprehend them before they achieve their objective.
- **Response** – procedures and actions for responding to a breach. Note: Because total protection is almost impossible to achieve, a security program that does not also incorporate detection and delay is incomplete. To be effective, all three concepts must be elements of a cycle that work together continuously.
- **Recovery** – your plan to continue business and operations as normally as possible following an incident. Mitigation planning is part of your response and recovery with the aim of minimizing the effects of any incident.
- **Re-assessment** – crucial and an ongoing process. Before implementing any changes, you need to revisit your strategic plan to ensure that goals and objectives will be met. Whenever there are changed circumstances or when new threats are identified, revisit your strategic plan and conduct a re-assessment to see what additional measures, if any, are needed.

You can now develop your own model secure facility. Work through the Assessment Checklist and answer each question by coming up with the most ideal solution. Not all the questions may be relevant to your facility, but for those that are refer to the answers below to assist you in coming up with your best solutions.