Security Executive Council

RISK MANAGEMENT PORTFOLIO

Physical Security Strategy and Process Playbook

John Kingsley-Hefty, Contributing Editor

Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

First published 2013

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-417227-2

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Sharing is Caring: Physical Security Strategy and Process Playbook

The *Physical Security Strategy and Process Playbook* concisely and comprehensively lays out the requirements of physical security management as a critical part of sound business management.

The book includes an explanation of basic physical security concepts; a description of the probable security risks for more than 40 functional areas in business; security performance guidelines along with a variety of supporting mitigation strategies; performance specifications for each of the recommended mitigation strategies; guidance on selecting, implementing, and evaluating a security system; and lists of available physical security resources.

You will find this playbook useful as you develop the functional requirements of a security system that meets your goals and fits within your business operations. These functional requirements are essential for receiving assistance from management, engineering, and finance. In addition, this playbook is a handy reference when you are planning for future changes.

Ways to use this resource:

- As a process reference for creating a physical security program
- As a primer for non-security personnel with a new security-related job responsibility
- To help a new security manager quickly define security requirements
- To help research solutions
- To help develop a request for engineering assistance and budget
- As a program gap analysis
- As a progress review or to assess the maturity of an existing program
- To help determine whether programs are adequately documented

Send feedback about this resource to: contact@secleader.com

CONTENTS

CHAPTER 3

Security Performance Guidelines and Options

3.1 INTRODUCTION

This chapter discusses the security performance guidelines and options relevant to each functional area of your business. These guidelines and options are meant to help you take action after you have reviewed the security risks to a particular area and have decided that the area does not have the appropriate level of security.

The functional areas in this chapter are arranged alphabetically, as in the previous chapter. For each area, the following information is given:

- Planning considerations
- Suggested minimum security requirements
- Recommended enhancements

Note: In this chapter, the suggested minimum security requirements for an area are indicated by a single check mark (✓). Recommended enhancements, on the other hand, are indicated by a double check mark (✓✓).

The security measures or options given for a specific area are designed to bring that area up to its appropriate level of security. The particular option you select depends on your facility and your business operations. In some cases, the suggested minimum requirements may be the best way to meet an area's security needs. The overall goal is to maintain a level of security that is most appropriate for each area of your business.

3.1.1 Performance Guidelines

In Chapter 1, we introduced the eight security performance guidelines that you need to be aware of (see Figure 3.1). These guidelines are the security goals for your organization's business operation and site.

Performance Guidelines	
1. Identify your security needs	5. Detect unauthorized access
2. Integrate security	6. Be prepared for an incident
3. Control physical access	7. Respond effectively
4. Control information access	8. Report promptly

Figure 3.1 Performance Guidelines.

3.2 FUNCTIONAL AREAS: GUIDELINES AND OPTIONS

The functional areas of your business are listed, in alphabetic order, in the following sections.[1] For each area, the following information is given:

- Planning considerations
- Suggested minimum security requirements (✓)
- Recommended enhancements (✓✓)

Keep in mind: a planning consideration that is common to every functional area included in this chapter is to review the performance guidelines in Figure 3.1and apply them appropriately.

3.2.1 Access Control for Property and Undeveloped Land

Planning Considerations

- Review your access control policy. Ensure compliance with your organization's access control and ID policy (see Chapter 1).
- What are the realistic types of threat to the facility?
- Assess the volume and composition of pedestrian traffic in the area.
- Will signs and clear perimeter lines control pedestrian walk-on?
- Do you need barriers, gates, fences, or berms to control access and circulation?
- How do visitors access the site? Do they need a separate access point?
- Is adequate parking provided in appropriate locations?
- Is it possible to light the site effectively?

[1]If you want to review the kinds of security risks associated with each area, please refer back to Chapter 2.

Suggested Minimum Security Requirements

- ✓ Use an environmental design that incorporates natural barriers and landscaping.
- ✓ Install signs of the right type in the right places to show the extent of your organization's property, the circulation pattern in effect, and any potential hazards on the property.
- ✓ Use lighting that conforms to national lighting standards.
- ✓ Minimize access and egress points.
- ✓ Use walkways, tunnels, and overpasses to avoid additional access points.
- ✓ If fencing is used, secure or control access to all gates.
- ✓ Perform routine inspections and provide an audit trail of all inspections.
- ✓ Be certain that you have the rights to inspect property and vehicles by posting the required signs.
- ✓ Park trucks, forklifts, and other vehicles away from fences and buildings so as to not provide assistance to those seeking unauthorized access to the facility. Be certain to remove the keys from all vehicles.

Recommended Enhancements

- ✓✓ Utilize electronic access control systems in conjunction with human oversight and involvement.
- ✓✓ Provide intrusion and unauthorized egress detection systems.

3.2.2 Access Control for a Site that is a Functioning Business Operation

Planning Considerations

- Review your access control policy. Ensure compliance with your organization's access control and ID policy (see Chapter 1).
- What are the realistic types of threat to the facility?
- Assess the volume and composition of pedestrian traffic in the area.
- Will signs and clear perimeter lines control pedestrian walk-on?
- Is it sufficient to have a set of restricted vehicle access points?
- Do you need barriers, gates, fences, or berms to control access and circulation?
- How do visitors access the site? Do they need a separate access point?
- Is adequate parking provided in appropriate locations?
- Is it possible to light the site effectively?

Suggested Minimum Security Requirements

- ✓ Use an environmental design that incorporates natural barriers and landscaping.
- ✓ Install signs of the right type in the right places to show the extent of your organization's property, the circulation pattern in effect, and any potential hazards on the property.
- ✓ Use lighting that conforms to national lighting standards
- ✓ Minimize access and egress points.
- ✓ Use walkways, tunnels, and overpasses to avoid additional access points.
- ✓ If fencing is used, secure or control access to all gates.
- ✓ Perform routine inspections and provide an audit trail of all inspections.
- ✓ Be certain that you have the rights to inspect property and vehicles by posting the required signs.
- ✓ Park trucks, forklifts, and other vehicles away from fences and buildings so as to not provide assistance to those seeking unauthorized access to the facility. Be certain to remove the keys from all vehicles.

Recommended Enhancements

- ✓✓ Utilize electronic access control systems in conjunction with human oversight and involvement.
- ✓✓ Provide intrusion and unauthorized egress detection systems.

3.2.3 Access Control for a Building or Part of a Building (see also Multiple Tenant Facilities)

Planning Considerations

- Review your access control policy. Ensure compliance with your organization's access control and ID policy (see Chapter 1).
- Not only must the perimeter be secured against unauthorized persons, it must also be secured against authorized persons gaining access at the wrong time or for the wrong reason.
- New business trends, such as the use of contract employees, contract manufacturing, and contracted services such as cleaning and trucking, produce a higher volume of individuals who are inside the facility. In addition, all these people have an extended group of friends, family, and other employees who know something about your site and who can test your security system.

- Integrate policies, procedures, and human intervention with technology to provide a secure building perimeter.
- The more openings in the building, the more difficult it is to control access.
- Do the number of access points meet the access requirements of the business? Are there too many?
- Where do visitors, employees, contractors, and service personnel enter the building?
- Are building, shipping, and receiving access points separated?
- Are the access points properly lighted to meet engineering's lighting standards?

Suggested Minimum Security Requirements

- ✓ Use an environmental design that incorporates natural barriers and landscaping.
- ✓ Install signs of the right type in the right places to show the extent of your organization's property, the circulation pattern in effect, and any potential hazards on the property.
- ✓ Use lighting that conforms to national lighting standards
- ✓ Minimize access and egress points.
- ✓ Provide intrusion and unauthorized egress detection systems.
- ✓ Use walkways, tunnels, and overpasses to avoid additional access points.
- ✓ If fencing is used, secure or control access to all gates.
- ✓ Perform routine inspections and provide an audit trail of all inspections.
- ✓ Be certain that you have the rights to inspect property and vehicles by posting the required signs.
- ✓ Park trucks, forklifts, and other vehicles away from fences and buildings so as to not provide assistance to those seeking unauthorized access to the facility. Be certain to remove the keys from all vehicles.
- ✓ Secure doors and windows against unauthorized entry and egress.
- ✓ Secure utility access points and other structures near a building to prevent their use for unauthorized entry.

Recommended Enhancements

- ✓✓ Use electronic access control systems in conjunction with human oversight and involvement.

✓✓ Provide CCTV camera and recording coverage at primary entry and egress points.
✓✓ Use an alarm system to annunciate unauthorized access and egress.

3.2.4 Building Services

Planning Considerations

- Control access and provide an audit trail to reduce the risks associated with the area.
- Minimize the number of entry points.
- Make an assessment of both the company and personnel providing the service and the degree of security necessary for meeting the performance guidelines.
- Consider the time of day the service is provided and the amount of supervision required when screening potential service vendors.
- Develop a contingency plan for dealing with a loss of service.

Suggested Minimum Security Requirements

✓ Use a list of preapproved personnel from the company providing the service.
✓ Establish and maintain procedures that keep current the list(s) of authorized personnel.
✓ Use locks and locking hardware, key control, and an audit trail for the area accessed by the service personnel.
✓ Post clear and obvious signs for restricted access and hazardous areas.
✓ Assign security responsibility to a single individual for each critical service.

Recommended Enhancements

✓✓ Restrict access to only those areas and times required for completion of installation, maintenance, and upgrade work.
✓✓ Use electronic access systems for areas with high personnel volumes or high personnel turnover.
✓✓ Use intrusion devices for areas that exceed safe levels of vulnerability or criticality.

3.2.5 Cafeteria

Planning Considerations

- It is critical that cafeterias are located within public areas of your facility. See *Public Spaces* in this chapter and *Adjacency Planning* in Chapter 1 for more information about planning for areas that contain or connect to public areas.
- The cafeteria's design should provide for a one-way flow of traffic from food selection to cashier.
- Provide an inventory storage space that has controlled and monitored access.
- There must be a safe or other secure container for storing receipts, or a bank-deposit procedure to eliminate cash security problems.

Suggested Minimum Security Requirements

- ✓ Control access to the dining areas if they provide access to an area that is not open to the public.
- ✓ Secure kitchen areas and stores during non-operational hours with a locking hardware system.
- ✓ Hold security reviews on contracted food services, both the contract employees and the contract itself.
- ✓ Provide for secure cash storage.
- ✓ Clearly sign areas that have restricted access or are hazardous.

Recommended Enhancements

- ✓✓ Use an electronic access control system where appropriate.

3.2.6 Cash Handling

Planning Considerations

- If the cash handling area is to be used by both employees and non-employees, locate the area in a public space. See *Public Spaces* for more information.
- Plan for secure cash storage and for low-risk cash transit.
- Review cash processing procedures so as to limit personnel involvement and minimize errors. Automate the process by using bar code scanning, payroll deductions, and other management techniques that remove cash from the system.

- Review your policies and procedures with internal auditing.
- If cash handling or cash storage amounts exceed $1,000, plan for intrusion and theft alarm systems.

Suggested Minimum Security Requirements

✓ Control access to the cash storage and cash processing areas such as cash rooms, cash machines, and storage containers.
✓ Use preemployment screening of all persons who will have responsibility for cash transactions and processing.
✓ Review your cash policies and procedures with internal auditing on a regular basis.
✓ Use locks and locking hardware, with key control and audit trails, to secure cash areas.

Recommended Enhancements

✓✓ For cash handling and storage areas that have amounts in excess of $1,000, install an alarm system that monitors and annunciates alarm conditions. See *Alarms Systems* in Chapter 4 for more information.
✓✓ Use recorded CCTV to monitor activity.

3.2.7 Chemicals

Planning Considerations

- Ensure that a review is conducted with the appropriate technical personnel so that the risks to this area are identified and minimized.
- Design the area to control access and contain spills.
- Develop operational procedures that establish adequate controls.
- Train your personnel and local emergency response units.

Suggested Minimum Security Requirements

✓ Use barriers to secure the areas where chemicals are stored.
✓ Post signs on all chemical storage areas.

Recommended Enhancements

✓✓ Use electronic access control systems.
✓✓ Install equipment that detects unauthorized access and that provides early warning/notification of releases or spills.

✓✓ Provide recorded CCTV to monitor access control points and other appropriate activity in the area.

3.2.8 Communications Equipment, Services, and Rooms

Planning Considerations

- Depending on your business, loss of phone service can be anything from an inconvenience to a devastating setback. Assess the criticality of phone service to your business and structure your security measures accordingly.
- Have in place procedures for temporary replacement of telephone services in case your system fails.
- Schedule phone system service, repairs, and upgrades during business hours whenever possible. Provide escorts for the service personnel.
- During the design phase, be certain to locate the telecommunication rooms away from areas where proprietary information or processes may inadvertently be exposed.
- Telecommunications areas are part of an interior concentric zone of protection, probably Zone 4, where only those people with a demonstrated business need are given authorized access.
- Doors, locking hardware, and construction must be designed to delay unauthorized access, allow for detection, and promote quick response.
- Plan for adequate environmental equipment such as uninterruptable power, heating, cooling, and humidity controls.
- Plan for access and audit controls that ensure preapproved, authorized nonemployees working in the area have an appropriate level of supervision.

Suggested Minimum Security Requirements

- ✓ Configure systems in accordance with IT, telecommunications, and your organization's security representative recommendations.
- ✓ Clearly sign areas of restricted access and hazardous areas.
- ✓ Control access to all interior equipment and provide an audit trail of access to the area.
- ✓ Escort visitors and employees as appropriate.
- ✓ Maintain an audit trail of all access activity into the area.
- ✓ Control access to all exterior equipment such as satellite ground stations, microwave parabolic reflectors, and communications towers/supports.

- ✓ Ensure that online information, passwords, and procedural controls are at a level consistent with the physical access controls.
- ✓ Develop operational security procedures in accordance with IT security's systems guidelines.

Recommended Enhancements

- ✓✓ Install recorded CCTV with video monitor and time/day/date recording capability to monitor the area and entrance(s) to the area.
- ✓✓ Use an alarm monitoring system. Provide for local response to alarms.
- ✓✓ Use electronic card access where appropriate.
- ✓✓ Control access to all interior spaces and equipment with remote management services (RMS) and CCTV and provide an electronic audit trail.

3.2.9 Computer Rooms

Planning Considerations

- Computer rooms are part of an interior concentric zone of protection, probably Zone 4, where only those people with a demonstrated business need are given authorized access.
- Prior to the purchase of security hardware and software, an evaluation of the security design features must be completed in conjunction with IT, telecommunications, and your organization's security representative.
- Doors, locking hardware, and construction must be designed to delay unauthorized access, allow for detection, and promote quick response.
- It may be critical that you have procedures in place for temporary replacement of computer services if your system fails.
- Plan for adequate environmental equipment such as uninterruptable power, heating, cooling, and humidity controls.
- Provide access procedures and audit controls that ensure preapproved authorized nonemployees working in the area have an appropriate level of supervision.
- Ensure that online information, passwords, and procedural controls are at a level consistent with the physical access controls.
- All operational security procedures must be in accordance with IT security systems guidelines.

Suggested Minimum Security Requirements

- ✓ Configure systems in accordance with IT, telecommunications, and your organization's security recommendations.
- ✓ Clearly sign areas of restricted access and hazardous areas.
- ✓ Control access to all interior equipment and provide an audit trail of all access to the area.
- ✓ Escort visitors and employees as appropriate.
- ✓ Use locks and locking hardware, along with the appropriate key control and audit trail procedures.

Recommended Enhancements

- ✓✓ Install recorded CCTV with video monitor and time/day/date recording capability to monitor the area.
- ✓✓ Use an alarm monitoring system. Provide for local response to alarms.
- ✓✓ Use electronic card access where appropriate.
- ✓✓ Control access to all interior spaces and equipment with RMS and CCTV and provide an electronic audit trail.
- ✓✓ Maintain an audit trail of all access activity into the area, during both business and non-business hours.

3.2.10 Construction Sites

Planning Considerations

- Determine how to define construction areas and how to segregate them from existing organization property and facilities.
- Limit entry and exit points.
- Plan for adequate lighting in compliance with national lighting standards.
- Plan for and design access control credentials and follow your organization's access control and ID policy (see Chapter 1).
- Define material, tool, and equipment requirements.
- Integrate control procedures for materials, tools, and equipment with existing operations.
- Plan for construction personnel parking. Minimize unnecessary vehicle entry/exit activity.

Suggested Minimum Security Requirements

- ✓ Provide temporary fencing.
- ✓ Provide a locking system that is keyed independently until the project is complete. Rekey the system so that it meets your organization's requirements at the time of your organization's acceptance and occupancy.
- ✓ Construction and service personnel must be trained in the site's safety and security requirements and procedures.

Recommended Enhancements

- ✓✓ Use a recorded CCTV system to monitor activity.
- ✓✓ Provide security patrols.
- ✓✓ Designate an organization security officer, organization employee, or contract security officer to control access and patrol the area.

3.2.11 Data Storage

Planning Considerations

- Physically locate on-site data storage areas as far away from IT (or information services) as possible.
- Plan for off-site storage, depending on the value, amount, and criticality of the data.
- Review your facilities for protection against the natural hazards appropriate for your geographic location (e.g., floods, earthquakes, tornadoes).
- Review your facilities and your security measures for protection against accidental damage due to fire, explosion, and structural collapse.
- Review your security measures to protect against human damage, both intentional and accidental (e.g., theft, destruction, tampering or modification, chemical spills).

Suggested Minimum Security Requirements

- ✓ Control access to minimize the number of people who access the area.
- ✓ Provide an audit trail of all access activity.
- ✓ Use smart locking systems, with key control or unique individual PINs providing audit trail.

✓ Design data storage containers specifically for protection against fire, theft, water damage, spills, and tampering.

Recommended Enhancements

✓✓ Use alarms systems with local annunciation and response.
✓✓ Use recorded CCTV to monitor activity.

3.2.12 Elevators

Planning Considerations

- Control access to elevator equipment rooms.
- Integrate elevator systems with security monitoring systems.
- Plan for controlled access where appropriate.
- Locate the elevator towers within the interior of the facility, preferably within a Zone 3 element.
- Plan to accommodate controlled public access.
- Isolate sensitive business areas away from elevators and their traffic patterns.

Suggested Minimum Security Requirements

✓ Control access during non-business hours when appropriate.
✓ Monitor for alarm conditions.
✓ Equip all elevators with emergency lighting and communications equipment.
✓ If your organization shares occupancy of a building with other businesses, maintain the necessary level of security through an access control system at a point before your organization's space is entered.

Recommended Enhancements

✓✓ Use electronic access control systems.
✓✓ Use recorded CCTV to monitor the elevators.
✓✓ If you want to use a keypad access control system, do not use a common code. Smart keypads with unique PINs or cards offer a more secure system.

3.2.13 Employee Store

Planning Considerations

- Plan for cash handling and cash holding areas.

- To protect inventory, plan for controlled access during non-business hours.
- Select a location next to or within a public space to restrict access to your organization's business space and operations.
- Provide direct access from the store to public facilities (restrooms, telephones, water fountains, vending machines, etc.)
- Review floor plan for customer traffic flow that's appropriate for the store's hours, location, and sales volume.
- If cash handling and storage exceed $1,000, plan for intrusion and theft alarm systems.

Suggested Minimum Security Requirements

- ✓ Post signs for personal use/no resale products, maximum quantity allowed, escort policy, restricted areas, and other information the customers need to know.
- ✓ Control after-hours access and provide an audit trail.
- ✓ Provide employees with training on cash handling, robbery, and theft procedures.
- ✓ Establish purchase records and log the frequency of restricted sale merchandise purchased by each customer.
- ✓ Place high-value, high-risk items in locations that will minimize shoplifting.
- ✓ Review cash handling and balancing procedures with internal audits for appropriate controls.
- ✓ Provide locking hardware and key control for the entrances and exits.

Recommended Enhancements

- ✓✓ Install recorded CCTV to monitor activity.
- ✓✓ Use electronic access systems for appropriate areas.

3.2.14 Entrances and Exits

Planning Considerations

- Your ability to control your building's entrances and exits depends on your access control methods. The probability of security incidents or losses resulting from unauthorized persons gaining access to a facility is greatly reduced by well-designed and frequently validated access

control methods. In addition, your methods must allow you to handle exceptions and to escalate security measures rapidly when necessary.
- Plan for alarm response. Your organization's policy should require controlled access and an audit trail.
- Design a limited number of active entrances and exits into the plan for your facility.
- In the design of an entrance, anticipate the peak periods of traffic and control.
- At facilities with 200 or more employees, consider separate entrances for visitors, employees, and services, to avoid conflicts in circulation and in access control.
- At manufacturing and distribution sites, consider separate and controlled entrances for shipping, receiving, and warehousing functions
- All exit-only doors must be used solely for exiting.
- Plan for integration of equipment and personnel to reduce costs and increase effectiveness.

Suggested Minimum Security Requirements

- ✓ Control access in accordance with your organization's policy.
- ✓ Use a badging system to meet access control requirements for both employees and nonemployees.
- ✓ Provide smart locking systems with key control and audit trail.
- ✓ Secure doors and post signs as necessary.
- ✓ Provide lighting in accordance with national lighting standards
- ✓ Use door seals or emergency exit alarms on exit-only doors.
- ✓ Escort visitors when appropriate. See Chapter 4, *Escort Policy*, for more information.
- ✓ Post clear signs at vehicle and pedestrian entrances and exits.
- ✓ To reduce the risk of unauthorized access, and to lower the costs of door hardware, eliminate exterior hardware from exit-only doors whenever possible.
- ✓ Review your procedures and inspect all entrances and exits frequently. Be certain to validate that all equipment, systems, and services are operating as designed.

Recommended Enhancements

- ✓✓ Provide recorded CCTV to monitor all access activity.
- ✓✓ Use electronic access control systems where appropriate.

ABOUT THE CONTRIBUTING EDITOR

John Kingsley-Hefty is an experienced security consultant whose leadership, accountability, communication skills, and project management experience in security, facility design, building types, operations, programs, and products has spearheaded team success stories for clients' critical corporate initiatives to advance growth and competitive advantage.

As a registered architect, John's strategic vision and planning reduces security costs by advancing security into the preliminary building design process. For over 35 years John has been successfully providing security and design services to diverse organizations such as 3M, Chicago Tribune Companies, and St. Jude Medical, Inc.

John's area of expertise is physical security architecture.

About Elsevier's Security Executive Council Risk Management Portfolio

Elsevier's Security Executive Council Risk Management Portfolio is the voice of the security leader. It equips executives, practitioners, and educators with research-based, proven information and practical solutions for successful security and risk management programs. This portfolio covers topics in the areas of risk mitigation and assessment, ideation and implementation, and professional development. It brings trusted operational research, risk management advice, tactics, and tools to business professionals. Previously available only to the Security Executive Council community, this content—covering corporate security, enterprise crisis management, global IT security, and more—provides real-world solutions and "how-to" applications. This portfolio enables business and security executives, security practitioners, and educators to implement new physical and digital risk management strategies and build successful security and risk management programs.

The Security Executive Council (www.securityexecutivecouncil.com) is a leading problem-solving research and services organization focused on helping businesses build value while improving their ability to effectively manage and mitigate risk. Drawing on the collective knowledge of a large community of successful security practitioners, experts, and strategic alliance partners, the Council develops strategy and insight and identifies proven practices that cannot be found anywhere else. Their research, services, and tools are focused on protecting people, brand, information, physical assets, and the bottom line.

Elsevier (www.elsevier.com) is an international multimedia publishing company that provides world-class information and innovative solutions tools. It is part of Reed Elsevier, a world-leading provider of professional information solutions in the science, medical, risk, legal, and business sectors.