Seven Spears Security International, LLC
Collaborative • Security • Solutions
Phone: +1.877.885.9141
Email: info@7SpearsSecurity.com

A Physical Security Primer for Executive Protection Professionals

By Seven Spears Security International, LLC

Introduction

When the term "*Physical Security*" is brought up in our industry, it is usually accompanied by a smirk or an eye roll. It is often deemed an "entry level" task that conjures images of *Paul Blart the Mall Cop*. No experienced professional would hang their hat on such a rudimentary function, would they? It has been our experience that physical security is often misunderstood and performed poorly. Yet, if the principles and concepts of physical security are understood fully and incorporated into the overall protection strategy appropriately (technology, intelligence, etc.), it can be just as critical a component as any other facet of protective operations.

Physical Security Defined

We need to start off with a common operating definition of physical security. There are as many sources for this as there are people to give their opinion. **Here are a few of our favorites:**

> **A)** *Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.* [Reference 1]
>
> **B)** *Physical security protects people, data, equipment, systems, facilities and company assets. Methods that physical security protects these assets is through site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection. Business continuity or disaster recovery plans are required to reduce business interruption in times of natural disaster, explosion or sabotage.* [Reference 2]
>
> **C)** *Physical security is a combination of physical and procedural measures designed to prevent or mitigate threats or attacks against people, information and assets. Often a measure designed to meet one particular physical security goal may address others. An effective physical security program has the aim to deter, detect, delay, respond and recover to planned and unplanned threats.* [Reference 3]

To summarize, we believe that Physical Security is the processes, procedures, and policies that effectively protect, prevent, respond, and recover from planned and unplanned events that could negatively impact critical assets or functions in a given location.

Preparation

Sounds daunting, right? So how is a cogent, comprehensive and effective physical security program achieved? Before we answer this question, we think it's important to first zoom-out a few magnifications and look at some big picture items. These preparatory steps are often overlooked or skipped, but they make a world of difference when you're trying to "eat this elephant" one bite at a time:

Step 1: Prepare Yourself

This step involves you, as the security practitioner and physical security expert, ensuring that you have the necessary training, licenses, knowledge, and insurances to be effective. This cannot be overemphasized. One assumes that the only thing required to implement "common sense solutions" is a bit of common sense. Unfortunately, we frequently encounter this misconception. However, as a professional you owe it to yourself, your client, and – frankly – the industry to set a higher bar. Get the necessary education and training to understand foundational concepts. Attend continuing education to keep up-to-date on industry best practices and improvements. Get licensed in the city/state/region where you are working. Obtain the necessary professional and liability insurances that not only "cover your butt" but show that you take your profession seriously. We could re-invent the wheel on this and expound more, but the experts at AS Solution covered it better than we could in their recent blog: *Licensing, liability and legal compliance issues in protective security: What high net worth families need to know*.

Step 2: Prepare Your Work

If you're anything like us, you hate sitting around talking about a job. "Let's just jump in and do it!" is our normal sentiment. We've hated homework since it was first assigned to us as children. However, it is important when conducting physical security assessments to slow down and do the preparation required. **There are several factors to consider in this category:**

1) Be culturally compliant

It would do us no good to recommend an 8-foot tall chain link fence with razor wire be emplaced as a perimeter security feature on the Google campus. It doesn't fit their culture. While this is an over-exaggeration to illustrate the point, it is important to understand the culture of the site you will be assessing.

Questions For Consideration

- Does the family estate, company campus, or satellite off-site want to appear "hardened" or do they want to have a welcoming and inviting appearance (with security personnel and features more "incognito")?

- Will employees be receptive to certain access control methods?

- Is your physical security assessment a priority to the client or a compliance issue being forced down their throat?

There are countless nuances that come into play as it relates to cultural sensitivity. And yes, while it all sounds like a bunch of "touchy feely" things that shouldn't concern you as a security practitioner, culture is critically important. It does no good to implement a robust physical security program that no one follows because it does not fit the culture of the environment.

Spend a few days on site. Get to know the people that work/play/live there. Understand what their tolerance level is and what their concerns are. This will pay huge dividends in the long run.

2) Identify "need to haves" versus "want to haves"

We run into this all the time. A security director will bring us in to consult on a given site. They will have an agenda of what they think should be identified and fixed. It's normally stuff that hasn't gained a lot of traction and the hope is that an outside opinion will get the process rolling. We obviously take the desires / wants of our client to heart. But it is important during the preparation stage to identify the key and critical assets that absolutely must be protected.

This helps you as you conduct your assessments, to prioritize your assessment efforts, your client's budget, and the mitigation measures that need to be implemented.

3) Have a quality control process

This is a critically important factor that is often overlooked in our industry.

Questions For Consideration

- Are your actions and recommendations compliant with industry best practices or ISO standards?
- Do you have processes to ensure quality control?
- Handle customer service complaints?
- Mid-project customer engagement strategies?
- Do you have established processes and procedures that follow the Plan, Do, Check, Act quality management cycle?

4) Conduct a Threat/Vulnerability Assessment (TVA)

What are the current threats and environmental considerations that could potentially impact the site that you are assessing?

In this category, practitioners will often jump right into categories of crime and terrorism. Yes, these are important. But it is also important to consider hazards relating to climate, labor union issues, political, infrastructure (power grid, water supply, etc.), and tangential issues.

Side note: Tangential issues are those which, while not directly related to your customer or site, may still affect it. An example we had recently was the declaration by the President of the US acknowledging Jerusalem as the capitol of Israel. This sparked protests all over the world, but specific to our client, the protests shut down the street where they were located. The anti-US sentiment was so strong that consideration needed to be taken on threats to the client simply because it was a US company, employee vehicle markings, etc.

Given the myriad of things that must be considered, now is probably a good time to pause and discuss the over-used and often misunderstood “All-Risk Approach” saying:

The All Risk Approach

One of the core tenets of modern risk management is the concept of “All-hazards” or “All-risk” planning. While a common phrase, few know how to properly implement this concept. Does all-risk planning mean we must plan for each one? The answer to this question is not as obvious as one would originally think. Many security practitioners believe that “all-risk” means planning for every possible eventuality and the contingency books/annexes tend to start stacking up. The simple fact is that “all-risk” planning under this precept is simply untenable. No organization or jurisdiction has sufficient resources to accomplish this effectively. Even if it were possible to foresee every hazard, Murphy still gets a vote at the table.

There are two key components to effective all-risk planning:

1. The first component is the concept of risk analysis.

Instead of dissipating limited planning resources on all possible hazards, risk analysis instead focuses on community vulnerability to specific risks. This allows planning resources to be dedicated to those risks (not hazards) that are most likely to affect the community. For example, rather than wasting resources analyzing the hazard of a tornado, a blizzard, and an earthquake; instead we focus on the risk of “loss of power” or “limited access to the facility,” regardless of the hazard that caused that risk.

2. The second component of all-risk planning is the development of the capacity to deal with multiple hazards through functional planning.

This is based on the assumption that certain core mitigation measures will apply to multiple incidents and a lot of risks are mitigated in the same way, be it through access control, perimeter security, technical security, etc. Building response *capacity* is a mitigation strategy that creates baseline capabilities that can not only deal with anticipated risk, but can be modified to deal with the unexpected.

All-risk planning is a sound and proven concept. But it does not mean that one must plan for every possible hazard. It does mean that one should consider all possible hazards as part of a risk analysis. Using a risk-based (not hazard-based) approach to planning, coupled with functional and prioritized contingency planning, we make the best possible use of limited resources.

5) Prepare your Risk Matrix

The final preparation step to developing a comprehensive physical security plan is to play the "what if" game with your key / critical assets. You need to assess the vulnerability of those assets against two categories: (1) The *most probable* incidents or threats that could occur and (2) The *most catastrophic* incidents or threats that could occur. What is the impact that these incidents will have on your key / critical assets? As you build this matrix, you will have to establish some baseline definitions on impacts and likelihood, as well as discuss whether certain assets need to be weighted more than others. Finally, you will develop mitigation measures to address these vulnerabilities and then re-assess the impact, once the mitigation measures are in place.

Execution

Let's recap. Up to this point, we've gotten educated, certified, and licensed. We've got enough insurance to cover us personally and professionally. We've spent our time doing the requisite preparation: We've got a good sense of what culturally will / won't work with our client. We've identified a QM process to ensure that we keep the customer engaged, updated, and the project on track. We've identified critical assets to the company and the most likely and most critical risks to those assets. We've taken into account Murphy and grouped risks together under common themes with similar mitigation strategies. Finally, we've developed mitigation steps to reduce our vulnerability to those risks.

Now, it's time for the real work to begin.

6) Start at the Top

Implementing a physical security program can be a daunting task. We like to start at the forest and work our way down towards the trees. That means that we start with policies and procedures. In the course of conducting your TVA, you should have identified missing or incomplete policies or procedures for the site.

There are countless ones that come to mind, but just to name a few: Vendor Access and Escort, Mail Handling, Bomb Threat, Fire, Evacuation, Media Storage and Security, …the list goes on.

Not all are applicable to every site, but don't dismiss a specific policy simply because there is the appearance that it wouldn't apply. For example, policy and procedure review in terms of Estate Security is often overlooked. However, if the threat is either more likely or the impacts are more critical at the home location, then there absolutely should be policies and procedures put into place.

What is important, is to evaluate the policies and procedures of a given location based on the following criteria:

Completeness

- Do they exist?
- Are they of sufficient scope/scale?
- Where applicable, do they conform with regulatory guidance?

Effectiveness

- Do they work?
- Have they been practiced/tested?
- Is there a cross-leveling of planning/execution/coordination between different business units/ verticals (legal/HR/PAO, etc.)?
- Are lessons learned re-inserted back into the process/policy/procedure?
- Are they in line with industry best practices?

Measurable

- Are metrics identified that provide quantifiable evidence of a policy's effectiveness (or lack thereof)?
- **Developed appropriately, metrics for security auditing is important for three reasons:**

  1) It sets a baseline standard to evaluate the performance of a given mitigation measure. Example: Safer Environment = happier, more efficient, more productive work force.

  2) It gives historical data used for comparison to evaluate the effectiveness of a security strategy, training event, or program (this speaks to the *Security Conundrum* – how to prove ROI when no security incidents occur).

  3) Effectively shaped metrics align with stakeholders' key business metrics to ensure security activities are in line with company vision and bring security from a cost center to a value enhancer.

Metrics can also help identify the level of risk being assumed if a security action is NOT taken, thus giving decision makers the information required to prioritize various initiatives or mitigation measures.

Bottom Line

Security metrics help practitioners answer the following questions with verifiable, quantifiable data:

A) Are the measures we recommend going to make us safer today than yesterday?

B) How does our physical security program compare with your counterparts'/competitors'?

C) Does this physical security program make you secure enough?

This could be a whole topic in and of itself, but we'll close the subject on metrics with this: security metrics should use the acronym **S.M.A.R.T.** (**S**pecific, **M**easurable, **A**ttainable, **R**epeatable, and **T**ime dependent).

The all-powerful dollar drives most high net worth families and nearly all businesses. When you can prove to your client how much money you saved them, compared to how much money they spent, you resonate with them in a language they are familiar with.

7) Work from the Outside-In

We are all familiar with the term *concentric rings of security.* This is a specific term that applies to physical security programs. Your outermost ring should be the one that addresses Threat Intelligence and Analysis. Having a codified program that gathers information on current threats and looks for emerging ones is critical to a proactive physical security program. Working our way in, perimeter security would be the next item to evaluate. Then grounds security, access control, safe rooms, personal security, etc. In each of these categories, we identify the most effective mitigation measures that address the most likely and the most critical risks.

8) Order of Work Priority

After conducting a full evaluation and coming up with a list of all mitigation steps, we then need to prioritize the order that the mitigation measures should be implemented. This priority should be done in conjunction with client input and with consideration on budgetary constraints, but should first address those steps that mitigate the most likely or most critical risks to the most vulnerable assets.

9) Don't Forget the Outliers

A mistake often made by physical security practitioners is to forget the elements that aren't within their direct scope of influence. It must be emphasized that, in the modern era, a comprehensive physical security program must integrate with technical security (cameras, drones, sensors, lighting, etc.), the Internet of Things (IoT), and cyber security.

Additionally, consideration must be given to the implementation of 3rd party assets. From an Estate Security perspective, that could mean giving additional training to an executive assistant, estate manager, housekeeper, nanny, or others on the premises to expand your capabilities.

Examples

- Can we teach the housekeeper how to handle mail appropriately?
- Can we teach the estate manager how to identify "suspicious behavior"?
- Can we give counter surveillance techniques to the nanny?

The same concepts hold true for any site. Providing training to a secretary on bomb threat procedures, giving additional duties to a person assigned as a Fire Marshall, giving extra medical training to a department…the list is endless. Don't forget to incorporate all the assets at your disposal into your physical security plans and procedures. When an incident occurs, the security practitioners will need all the help they can get!

10) Criminal Prevention Through Environmental Design (CPTED)

It is worth a brief mention on this subject that CPTED should be incorporated into your physical security program. Simply put, this means that you design mitigation measures in such a way so as to blend in with the environment. Not everyone wants their sites to look like a fortress! This could mean big things such as blast-proof tinting on windows, strategically planting trash receptacles to double as blocking devices for traffic flow, landscape lighting, etc. It can also incorporate concepts of how the furniture is arranged in a room to limit movement (but not impede work flow), in case of a workplace violence or active shooter scenario. Incorporating CPTED concepts into your physical security methods gives that "extra touch" your clients will appreciate that alleviates their worries of what the "security guy" is going to come up with.

Post-Execution

Now that you have conducted all of your assessments, created and implemented your plan, you're done…right? Wrong.

Now comes the most important (and often least conducted) element of physical security. Plans should be tested, evaluated, and lessons-learned reinserted back into the physical security cycle. These tests can be leadership "table-top" exercises, business continuity committees, key leader drills conducted after hours, or full-blown scenario drills that incorporate the entire workforce during the work day.

When conducting evaluations, it is critical to first gain leadership buy-in. These drills should NEVER be a surprise to the C-Suite. Each drill should have a specific goal to achieve and be objective in their evaluation. Post-mortem briefings should be given, which allow everyone to give their perspec-

-tive and input, and have timely feedback given to the key leaders. This feedback should not only address issues that need to be corrected, but also highlight positive things that should be sustained. All of this should be documented carefully and incorporated and memorialized to influence future metrics, policies and procedures.

Summary

When properly executed, physical security can be an involved and complex process that supersedes its seemingly simple reputation. There is a lot that goes into ensuring that a physical security program is comprehensive and effective. This primer was meant to introduce the basic concepts required to start a proper physical security program. However, this is just the beginning. Integrating physical security into technical and cyber security is a topic wholly on its own and is critical in this modern era. Crisis Contingency Planning, Business Continuity Planning and Security Audits are all advanced topics which have their roots in physical security.

About the Authors

MEB WEST CPP, CSS, CCM

Meb West is a retired Army Ranger, Intelligence Specialist and decorated combat veteran of both OEF and OIF. As a security specialist, Meb has extensive experience consulting on Security Compliance Management (SCM); auditing security policies, procedures, and programs for large, multi-national organizations. He specializes in conducting New Market Entry security advances in both domestic and international arenas. He has conducted Risk Assessments (RA) and Business Impact Analysis (BIA) for Business Continuity Management Teams and steering committees with operations that span the globe, and has provided asset and personal protection to clients in Africa and the Middle East. In each of these dynamic environments his number one goal is to find innovative ways to make the client smile; to turn the cost of security into an investment that creates tangible value.

JENNY WEST

Jenny is an Army Veteran and military spouse with over two decades of experience owning and managing small-to-medium sized companies. As an award-winning business owner, she has set her sights on the improvement of her local community by founding and managing a networking coalition of over 1,000 diverse businesses. Jenny is passionate about customer service and her professionalism is world class. When it comes to security, Jenny has a global eye on challenges – particularly those that pertain to women and families. This concentration originates from her many postings overseas where she lived and raised her daughter.

Sources

1. http://searchsecurity.techtarget.com/definition/physical-security
2. Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill;
3. https://www.protectivesecurity.govt.nz/home/physical-security-management-protocol/physical-security-management-protocol-2/introduction-3/definition-of-physical-security/
4. http://www.govtech.com/em/emergency-blogs/managing-crisis/Allhazards-Doesnt-Mean-Plan-for-Everything.html