The 7 Most Critical Considerations for Physical Security Systems

As a premier physical security consultant for governments and commercial enterprises, Kline Technical Consulting (KTC) has decades of experience determining the must-haves for reliable security systems. The best physical security systems use an integrated system of technology, staff, and communication to prevent unauthorized personnel from accessing a specific location or resource. This white paper will discuss the seven most critical considerations for planning, executing, and maintaining a robust and efficient security and communication infrastructure, including:

Consideration #1: Requirements Definition
Consideration #2: Cost
Consideration #3: Ease of Installation and Maintenance
Consideration #4: Disruption of Process
Consideration #5: Overt and Covert Systems
Consideration #6: Complexity of Control Functions
Consideration #7: Flexibility and Scalability
The 7 Most Critical Considerations for Physical Security Systems

When a breach in security occurs, civilians, politicians, and the military all want to know what went wrong and, more importantly, how the breach can be prevented next time. Regardless of whether the protection is for the nation’s leadership, a critical national resource, or an elementary school, decision makers need to methodically address these seven considerations to create an efficient and comprehensive security plan.

Consideration #1: Requirements Definition

Determining to what extent a subject will be protected is the first and most important step of building a physical security system, and it directly affects the second greatest concern, cost. The major parameters to establish when defining requirements include:

**Threat**
What are the general and specific threats? For example, if a bomb is stored in a bunker, the physical security system must block a threat of theft.

**Vulnerabilities**
What are the vulnerabilities against the threat? Vulnerabilities are driven by the value and nature of the protected subject. For example, depending on the size of the bomb, you may need to guard against different types of vulnerabilities. If the bomb is large, you need a truck to transport it, but if the bomb is small, you need only a purse.

**Value of Asset(s)**
What is the value of the thing that needs protection? The value of life is impossible to determine, but the gold in Fort Knox has a set value. The value of an object also varies in terms of its cost of goods sold versus its market value. A nuclear weapon may take $1 billion to build, but it may be worth $10 billion to a terrorist on the black market.

**Impact of Failure**
If the physical security system fails, how does this impact mission success, preservation of life or property, and so on? For example, a counterinsurgency operation affecting national security may require a radio antenna. The antenna is a simple part that can be purchased cheaply from Radio Shack, but it is essential for the mission – its failure could directly impact the nation’s security and jeopardize the lives of its people.

In order to properly design a physical security system, the specific problem and the value of defeating that problem must be defined. Contemplating threat and vulnerability helps the planner grasp the overall problem, while understanding the value of assets and impact of failure helps the planner rank different security concerns to ensure focus on the most important, more critical ones before addressing ones that are less critical. These four factors all affect the cost-benefit analysis of success, so that the planner can determine if it is worth spending $100 million protecting a base with only $5 million worth of property.

**Case Study: A Nation’s Largest Oil Refining Asset**
Take this hypothetical illustration of a country’s largest oil refinery that receives oil from tankers via an ocean port, and then transports the finished product by land via a railway and three...
major highways. Protection would encompass the refinery, storage tanks, dispersing stations, transportation routes, and other assets. The four main factors can be summarized as such:

**Threat**
The loss of refined product, money to dependent industries, and the refinery itself as an asset are all reasons for protecting the refinery.

**Vulnerabilities**
This country has a long-standing rivalry with a neighboring country, and therefore could potentially be subject to air weapons, missiles, rocket launchers, and low-altitude attack. Ocean attacks are also a possibility.

**Value**
This country wants to be self-sufficient for all its future fuel needs, so this refinery is a vital part of those plans and is deemed to be as important as protecting the president’s house. The refinery does not have many employees on site, but human life is still a source of concern. The loss of property, such as the equipment and railway, is also very important and would cost $150 billion to rebuild.

**Impact of Failure**
A breach in security would affect the reputation and pride of the nation. Unlike a nuclear weapon, the country would not be destroyed and the government can survive without it, but it would disrupt the supply chain of fuel. The ripple effect would be moderate to severe in terms of national security.

No single security plan can account for all situations in a cost-effective, sustainable way. Requirements definition serves to establish the specific thing to be protected and the ways it will be protected. Furthermore, every one of the conditions in the requirements definition needs to be stated and defined from the same point of view. Often, plans start off with a shaky concept, where the top two important must-haves from each department head in the organization are smashed together, creating a fragmented proposal. Instead, these ideas should be restated from a single perspective, such as the president’s perspective or primary user’s perspective to establish consistency.

Figure 1: Protecting a major resource such as a nation’s largest oil refinery starts with a requirements document to establish the importance of the asset and the details of the security plan.
Defining the Details
Using sufficient detail in defining requirements is critical to the success and execution of the plan. Let’s say a security officer is responsible the requirement, “There should be a visual or camera corridor on every aspect of the property, so that every part of the perimeter can be viewed all at once or panoramically.” This may appear to be a straightforward statement, but many details are still missing:

- Should the monitoring occur for 24 hours a day? If so, thermal cameras may need to be included.
- Does “can be viewed” mean the ability to notice something general or to study specific detail? The operator may notice something at the fence, but would require a variable zoom in order to identify the object. In order to follow an intruder once he or she moves 3 feet from the fence, the camera also needs pan and tilt capabilities.
- What about recording? Does the footage need to cover 100 percent of the time and how long should it be kept?

Depending on the answers to the detailed questions, the initial requirements could define a low-cost, standard system, or a very expensive integration suite with digital and analog data, high-accuracy signal conditioning, and a control room with input and output signals. As you can see, going through the definition process brings up new elements that will affect cost.

**Consideration #2: Cost**

Once you establish the project scope and plan, you can determine the cost of the physical security system and compare it to the actual item under protection. Cost is the bottom line for many planners, but focusing on cost alone can be a seductive trap to trust. Cost has many different definitions depending on the group’s point of view – the cost to equip and install the system, the cost to train and operate, the cost of quality, the cost and potential ramifications of failure, and so on. Consider these example costs and concerns from different affected groups all concerned about the same security system:

**For the Decision Maker**
The most important cost is **proven/expected security** – what will the security system keep out and what undesired intrusions may slip through?

**For the Workers Staff (those inside the building)**
They prefer a combination of what is **least cumbersome in operation** and what degrades their work efficiency the least – how much will these extra security measures and reviews slow down, interrupt, or obstruct my work?

**For the Security Officer**
He or she is likely focused on **efficiency** – how can we succeed without adding too many additional staff members, which drives up cost?

**For Visitors (such as vendors delivering products to the compound)**
They need to be able to come and go from the site easily – what has the **least inconvenience** for us to enter and leave the premise?

**For the Auditor**
The **cost per unit time** versus the **cost of failure** is an important factor – what is the risk in relation to cost?

**For the Politicians**
They are often concerned with approval – how will these additional measures affect my **reputation and ratings**?

**Learning from Real-World Security Failures**
With the increased visibility and flow of information in the media, failures in security become glaring public mistakes for all to see. The attack on the American diplomatic mission at Benghazi, Libya and the shooting at Sandy Hook Elementary School in Connecticut may seem like two separate tragedies, but the commonality is that neither the U.S. Secretary of State nor the Newtown Public School District was successful in providing security. This does not mean that the authorities were not paying for security measures or did not have written plans. However, there are many different users within a school district or the office of the Secretary of State. And within each unit, there are several paradigms that should be followed to most efficiently build a security system and its budget:

**Same Point of View**
From year to year, budget to budget, staff to staff, and so on, you must maintain the same point of view in order to accurately analyze the security program’s cost and effectiveness. For example, a principal at a school could be the arbiter of the cost of security. As changes are suggested or removed each year, the security plan must be evaluated from the point of view, requirements, and trade-offs on cost versus performance that the principal originally evaluated.

The same principle applies to a much larger scale, U.S. national security. Is it from the point of view from the president, the Secretary of Defense, or Department of Homeland Security? Each of these people or groups talk about “security” without defining their
points of view, which can make it difficult to define, assess, and improve from year to year.

**Same Cost Element**

Just as it’s important to establish a single point of view when looking forward or looking back, you also need to stick to the same cost element or definition, a prioritized aspect of the security program and its cost. For instance, for a security system based on alerts, you hire good operators who can make quick judgments aided by cameras that have visibility over the area of protection.

In the U.S., everyone, from politicians to the public to the media, feels empowered to issue accolades or criticisms about different situations and events. With the attack on the Benghazi mission, the public asks questions about whether too few or too many people and procedures were in place, or if too much or too little money was spent on security. Just as saving cost is a number-one concern when building a security system, blaming cost is a number-one accusation when a security system fails. So, it is critical to define requirements specifically and control costs wisely so that designers and planners, who are constrained by a limited budget, can prioritize and protect spending on the most important aspects of the system.

**Consideration #3: Ease of Installation and Maintenance**

The difficulty of installing and maintaining the physical security system can introduce multiple layers of complexity. Security holes can temporarily increase during installation and maintenance of the system, so speed is of the essence. However, making choices solely based on how fast a system can be installed may increase maintenance costs in the long run. For example, if a requirements document includes 100 percent visibility of a site perimeter, 24 hours a day, you can use either portable cameras or hard-wired cameras. Portable cameras are much faster to setup, but outsiders can easily tamper with them by cutting wires or knocking the camera down, creating security vulnerabilities and adding repair costs. However, if you use concrete to bury the cable, the system requires almost no maintenance in the future but the installation will take several extra weeks.
Case Study: Multi-Stage Security for a Nuclear Plant

Another factor to keep in mind is that protecting complex facilities or subjects may require that installation is completed in stages with requirements defined for each stage. Take the example of providing security for a nuclear plant built from ground up:

Stage 1: While the Facility is Built
- The perimeter – which will be quite large at first – must be secured
- Vehicles coming in and out of the construction site need inspection
- Contractors that remain inside the facility need a second, separate method of inspection
- Once the nuclear plant has control ponds, those require some form of low-level protection
- Rod cooling tanks, which are normally outside the facility, require exterior security

Stage 2: After the Facility is Built
- More stringent security within the buildings must be set up to protect the reactor vessels and the control room
- Hierarchically linked security zones must be established as additional buildings are erected
- During the construction of the reactor vessels, the outer security will need to be changed.
- Access routes such as a railway entrance may be closed off
- The number of people inside the facility may be halved during the building of the vessels, so there will be a smaller, tighter perimeter to protect

Throughout the long process of building a nuclear plant, each security element should be examined from the standpoint of ease versus difficulty in its construction, implementation, and the maintenance that the plant will need throughout its lifetime.

Consideration #4: Disruption of Process

The security system must be flexible and comprehensive enough to account for all the procedural activities of a facility. In other words, during the regular operation of a facility, certain security activities may change the routine flow of people and materials. Therefore, the security plan must define elements that take into consideration the people and routine procedures at the facility, which may be disrupted by the security process.

Case Study: Deploying an Aircraft Carrier

Given the enormous size of an aircraft carrier, there is no disguising its presence at a port and therefore from a security standpoint, there is no point in trying to cover it up. However, concealing the activities and contents on the carrier is of utmost importance, so officials will execute special security plans that ultimately disrupt the normal operations of the dock. Besides managing the installation and operation of the temporary security plan and its disruptions, organizing the personnel logistics can become complex very quickly.
Six to eight weeks before departure, the usual crane operators and truck drivers are cleared from the dock. Since these dock employees are still on the payroll, they need to be kept busy working on something else, somewhere else. Then, a different set of people come in to load the carrier, set up and operate the physical security system, and guard the newly defined perimeter. The actual outer perimeter around an in-port aircraft carrier may be up to the size of a small town in Colorado.

Case Study: Installing Bank Security or Residential Security
On a much smaller scale, the same type of disruption of process occurs when building a bank. When it comes time to integrate the security control system, everyone is excluded from the location for several days. Only the specific contractor in charge of installation is allowed on-site. The windows are covered with canvas and workers can enter through only one door. All items – from the tools to the equipment to lunches – are brought inside using large footlocker containers so that their contents are not visible to outsiders.

If the security system is for a safe room for a government official’s residence, the planners may even go as far as stopping traffic from running in that neighborhood while the installation is occurring. The cost of interrupting or hindering the status quo, even for a temporary period, must be considered when designing a physical security system.

Consideration #5: Overt and Covert Systems
The desired visible level of security has some interesting psychological ramifications when it comes to deterring intruders. You want the terrorists or opposing forces (OPFOR) to see some security elements, such as guns mounted on the wall, because these overt systems will discourage a certain number of casual trespassers. The more experienced and resolved attackers will be looking for the hidden assets, in which case the physical assets in plain sight will catch them using their binoculars or small, portable radio systems. Ideally, the overt and covert systems should work together to reinforce one another.
In fact, overt and covert sensors often coexist. People expect to see some security elements, such as a camera mounted above a doorway, and may think nothing of it, but that same camera may contain a couple of radiation and magnetic sensors. Just because a sensor is concealed does not mean it has to be 20 feet away from the subject. It can be housed in the same chassis as the camera the person is walking past.

**Case Study: Detecting a Pack of Wolves or Humans**

Suppose the area around a classified compound has been mapped out with an array of microphones and sensors. These microphones can sense a wolf walking through the woods, record the sound signals, and send the data to computers for analysis. Motion is detected at 3 a.m., but the signal spectrum and time of night does not match the wolf pack’s patterns, so an operator turns on another bank of covert sensors hidden in the trees.

**Cost of Overt vs. Covert Systems**

In general, covert assets are more expensive because the hardware itself is pricier or the cost of installation is higher. An overt security system – comprising 2000 cameras, electric fences, underground concrete, tension wires, etc. – may cost $250 million, whereas the covert component – such as pressure sensors, sound sensors, assets in the air looking down with infrared, etc. – may be closer to $1 billion. Whenever possible, try to push things to overt systems to keep the expenses down, but still include enough covert systems to keep enemies unaware and uncertain.

**Consideration #6: Complexity of Control Functions**

The public thinks of security as a security officer in a guardhouse with multiple viewing monitors, and that the extent of the control functions is a large red button on the wall or counter for the guard to push if he sees something suspicious. In reality, control functions in a security system can be as simple as closing doors remotely to as complex as resetting all security levels in a compound within seconds of receiving an alarm.

The command center must handle a wide variety of control functions. The control functions for locking a door are different from those that control a camera. Even seemingly similar functions, such as controlling a valve for stun gas versus lethal gas, can be very different because of the
number of overrides in place as a function moves toward deadliness. Even if the functions are analogous, they may have dissimilar purposes and control logic behind them. For example, security for a prison has many of the same elements as security for a government compound, but some of the operating requirements are quite the opposite. In the government facility, the focus is on closely examining people and materials entering the building, but less focus is placed on those leaving. The opposite is often true for a prison.

**Case Study: In Case of Fire**

Fire control systems are a classic example of controlling security in different situations, because different doors lock and are left open based on what triggered the alarm. A less urgent, Stage 1 response may occur when a smoke alarm sets off a fire alarm, whereas a more urgent, Stage 2 response – for locking off areas with explosives, spent radiation units, or prisoners – may be used if the chief of security sets off the alarm.

Another level of complexity is to determine if the facility should have a fail-safe system or a fail-secure system. In a fail-safe system, all the doors can act as fire escapes and be opened to the outside, even if they’re normally locked. In a fail-secure system, certain doors will remain locked in the case of a fire, either to protect the contents inside or to route people to a certain location. For example, if there is a fire in a jail, you want to get people out of the building quickly but ensure that they are not released from the prison grounds into the outside world.

**Complexity of Control Functions Affects Reliability**

In general, as the SCADA system and control functions increase in cost and complexity, system reliability decreases. If you have a simple camera for a grocery store, it has a single feed and basic on/off control. If the camera is not working, most likely the battery failed. However, if the camera is for a classified area, there may be multiple sensors and alarm triggers, certain times when the camera should be turned off, and a list of people who may or may not be authorized to view the camera output. Any number of electrical and mechanical problems could cause a failure in the system. Therefore, carefully consider the difficulty and sophistication of your control functions in terms of reliability and mean time between failure (MTBF). The simplest solution often saves a lot of headache in planning and upkeep.
Consideration #7: Flexibility and Scalability

Few organizations enjoy a consistent, long-term mission and space – most have to change in size and often in scope. This means the security system must also be capable of extensibility, repositioning, and resizing. As you add areas – or even areas within areas – of protection, the redesign and rebuild of the control system can be extremely time consuming and difficult. To create successful security systems, you must plan for the most stringent and extended program, giving what you design room to grow in size and specificity.

Case Study: Flexible Security for a Port

When constructing a new port, the initial perimeter may require a two- to five-mile diameter of physical security. Control system boxes and cameras in vans monitor the concrete trucks and other construction vehicles at ingress and egress points. The outer perimeter generally has the least security and is less dense in terms of signals. As the port is built, the physical security system expands to protect the perimeter of the port, including the custom houses, storage warehouses, and so on. Ideally, the physical security system can be extended or shrunken, so invisible microwave fences may be used with portable tripod stakes so that they can be easily moved around as needed. Also, since the construction phase is temporary, cheaper security elements with relatively short lifetimes may be used and then removed to save costs.

Once the port is complete, the physical security system needs to protect and examine goods transferred in and out of the dock. Trains deliver goods to the outer perimeter of Security Level 1, consisting of railways and giant gantry systems. Once the goods are disgorged, they enter the smaller ring of Security Level 2 for closer inspection. As the items are moved around the port, workers stack them in large containers. The individual containers are determined to be safe, and are considered at the same level of security. However, the stacked containers create a large, maze-like environment that extends for thousands of feet, which can offer a lot of places for hiding explosives or terrorists waiting to plant bombs or even stow away. This presents a new security concern that didn’t exist before and must be addressed.

Taxed items may be rerouted and undergo further examination in a warehouse in Security Level 3 if something suspicious is detected, such as a small amount of radiation or an error with the paperwork. Finally, the smallest perimeter of Security Level 4 surrounds the control center. Everything between Security Levels 1 and 4 must connect and communicate directly with the Security Level 4 control center.
As the perimeter grows inward from construction to completion, the control system must be able to extend so that the operators are always using the same control interfaces and algorithms. The same types of control system boxes that were located inside vans during the construction of the port now are installed in the control center.

**Final Thoughts**

Ultimately, designing a security system involves a calculated gamble. How much are you willing risk in order to protect something? If the item is a nuclear weapon, the political impact of its theft and mortality impact of its usage makes it a prime example of when to error on the side of more security. If the subject is the Washington Monument, the monetary value is not ruinously high but its worth as a national symbol increases its importance. If the target is a train transporting concrete and sulfur, the low-risk scenario may drive the railway company to implement guards with flashlights and communicators to call the police.

Many decision makers are involved in the process of determining how important something is in terms of security. In the best case scenario, the attack never happens. For all other scenarios, carefully consider these top seven critical elements to implement a well-thought-out and highly effective physical security system.

**About Kline Technical Consulting**

KTC brings a unique combination of warrior, academic, and technical expertise to develop and field advanced security solutions. Its experienced military and engineering specialists work covertly and confidentially to create, develop and install tools, technologies and systems front line warriors need to survive and win.

For more information, visit klinenm.com/services/physical-security-systems.