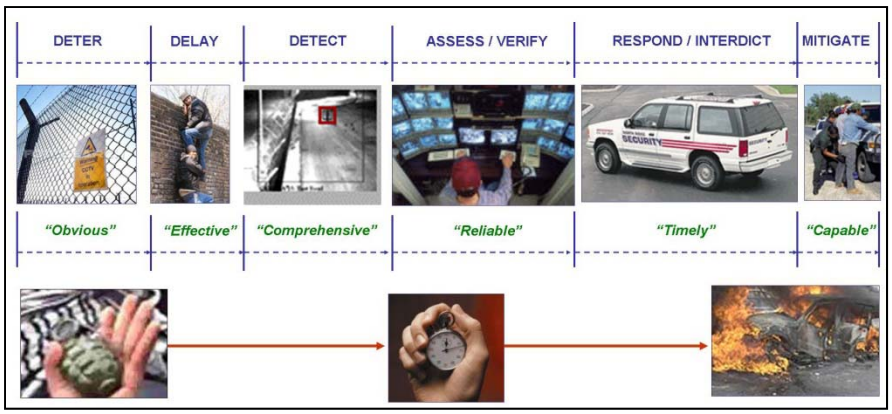
Why EFFECTIVE Physical Security is Inherently Tri-Dimensional

Minieri Associates
Security Consulting & Engineering Worldwide



By:

Michael Minieri, CPP

mminieri@minieriassociates.com

26 July 2014

"3D SECURITY: *Why Effective Physical Security is Inherently Tri-Dimensional*"

By Michael Minieri, CPP, CST, CCO, CET, CFPS, CPOI, CSM, RAM

Everyday around the globe, many organizations release solicitations for security devices and systems such as CCTC, Access Control, Guard Services, Screening Machines, Physical Barriers and the full range of available security products and services. Simultaneously, the media presents snippets of incidents where security measures were breached by ordinary people with little or no effort. Top executives might rightly question why, after investing millions on security, did this happen? In this article, Michael Minieri, a 40 year industry professional and Principal with Minieri Associates Worldwide Security Consultants, explains the underlying reason from his observations in nearly 30 countries.

According to a Washington Post article (7 Dec 2009), the U.S. Secret Service documented 91 breaches of security at the White House since 1980. Most would argue that 1600 Pennsylvania Avenue is generally considered one of the most secure facilities on the planet, and one can only imagine what their real security budget might be. BBC news (26 May 2000) reported that the U.S. General Accounting Office (GAO) was able to get past security at 19 federal buildings including the FBI, the CIA, the Pentagon and 2 of the country's busiest airports. Masada, an ancient, mountain top fortification established in first century BCE, was generally considered "impregnable", yet it was repeatedly defeated by a host of various adversaries throughout its history. Where might most of the existing security measures today fit in context of "high-security" facilities such as these? How does your facility compare?

"*Do you know if anyone is breaching your perimeter barrier RIGHT NOW?"* the Security Consultant asked the Security Manager during a meeting inside the latter's secured facility. The manager's facial expression conveyed the answer as one that was already known to the consultant. Perhaps no one ever asked that particular question before. Like MANY in similar positions, the Security Manager had a certain comfort level from the 10' fence topped by three strands of barbed wire angled 45 degrees outward. Besides, in his 18 years at the facility, there had NEVER been a breach of that perimeter to his knowledge.

The discussion continued; *"If an armed adversary gets feet on the ground inside your perimeter and runs for your toxic chemical storage tank with the intention of causing a release, what do you think would be the chances that your existing security measures will prevent a successful attack?"* was the next question. Same reaction.

Ultimately, the circumstances were as the consultant had expected based upon even casual observations when entering the facility, and after having observed many hundreds of similar situations across the globe. The facility HAS physical barriers, it HAS CCTV and it HAS a large guard force…but those 3 measures are not effectively "integrated". The facility DOES have "*security*", but it lacks "*effective security*". ***The 3 Essential Elements of Effective Security*** are Architectural security, Operational security and Technological security. His barriers, guards and cameras are examples respectively.

ARCHITECTURAL SECURITY includes physical components and facility design characteristics such as distances (like set back), the flow and traffic patterns of pedestrians and vehicles, the locations of mail and other delivery handling and storage, structural elements including glazing, concealment, lighting, proximity and similar aspects. Many architectural elements cannot be easily or economically altered after construction, such as the location of a fuel tank in close proximity to a perimeter fence.

OPERATIONAL SECURITY is about *people*, both security staff and everyone else that may come upon the premises. The core of this element is comprised of written policies, procedures, training, post orders, guidelines, rules, regulations, guard deployment strategy, staffing levels, emergency plans, reports and record keeping, drills and exercises, communications and other less tangible issues related to human behavior.

TECHNOLOGICAL SECURITY encompasses all "security purpose specific" systems and devices either off-the-shelf or fabricated for the intended application. Naturally, this includes common items such as CCTV, alarms, access control, dynamic vehicular barriers, etc.

These are the three dimensions (3D) of effective physical security. To achieve effective security, all three elements MUST be present and they MUST be properly integrated so that they work together as a single, cohesive and unified "security program".

Here's why; anyone – criminal, terrorist, employee, visitor or vendor – that intends to cause a loss to any asset is the "adversary" of the security program. Unlike law enforcement where the performance metric is *crimes solved by arrest*, the ultimate objective of any security program is to *prevent, reduce or otherwise mitigate potential losses*. To accomplish THIS objective, the 3 essential elements described must be integrated so as to provide **the *5 Essential Components of Effective Security***;

1. DELAY – "Time" is a CRITICAL factor. The adversary's progress toward the target asset must be impeded sufficiently long enough to "detect" (discover) the attack and to implement the appropriate response. This is the ONLY function of physical barriers (Architectural Security) since no barrier can prevent eventual entry by a determined adversary.

2. DETECTION – If one does not KNOW that an adversary is in the process of attacking, one has almost NO CHANCE of preventing or mitigating the potential loss. Various types of alarms and/or CCTV with video analytic detection (Technological Security) are commonly used for this purpose.

3. VERIFICATION – Since most "detections" ultimately prove to be from something OTHER THAN an actual attack (i.e. "false alarm"), it is necessary to verify (validate) an actual attack prior to initiating a response. Otherwise security staff "complacency" will eventually sabotage the effectiveness of the security program. CCTV (Technological Security) is generally the best method of accomplishing this, particularly since it can also serve in the "detection" capacity simultaneously.

4. INTERDICTION (Response) – In almost all cases, action must be taken that will position appropriate forces (Operational Security) somewhere along the adversaries path of travel to the target asset BEFORE the adversary reaches the asset. "Time, Speed and Distance" for both the adversary and the response force are critical considerations in security planning.

5. MITIGATION – The response force (Operational Security) confronting the adversary MUST be fully prepared and capable of preventing or otherwise mitigating the potential loss. This implies that the response force must be adequately TRAINED and EQUIPED for the circumstances. Perhaps its time to think about how those unarmed guards will protect against an armed adversary.

How "essential" are these 5 components? Omit or fail at ANY ONE and the unwanted loss to the target asset is all but absolute! Some will argue that "Intelligence" (advanced knowledge) and "Deterrence" should be included. They are not included as "essentials" because one rarely has actionable intelligence and if deterrence were ALWAYS effective, there would be no need for the remainder of the security measures. These are not controllable and therefore not *essential*. Another component might be "post-incident analysis" where one attempts to learn and improve through retrospective evaluation after every security incident. These are world-class, best practices, but they are not absolutely *essential*.

Consider the discussion with the Security Manager about an attack on his toxic chemical storage tank as an example. Our adversary – a disgruntled former employee - has a handgun, a small, crude explosive device, and starts from a point outside the perimeter barrier in this scenario;

A. The adversary drives his pickup truck on the public roadway to within a few feet of the perimeter barrier, climbs on the truck's roof, throws a heavy rubber or leather pad onto the barbed wire, and thereby defeats the barrier. This can be done is well under 1 minute. The CCTV video motion detection system causes an audible alarm in the security command center and displays the appropriate camera on the large, primary monitor for the security console operator.

B. The adversary runs full speed (*use 35ft or 10m per second*) toward the toxic chemical storage tank and a PTZ camera automatically tracks him. The attack is now visually verified and the console operator dispatches the response force via two-way radio.

C. The response force travels to the chemical tank and takes up defensive positions.

D. The adversary, faced with overwhelming and clearly superior counter-forces, drops his weapons and surrenders!

Maybe that IS "textbook"….but it's NOT "fairy tale book"! If this description is NOT close to the vision you have for your existing security program under similar conditions, is your current Security Master Plan likely to result in this same conclusion? Conceptually, the *3 Essential Elements* and the *5 Essential Components* are applicable to the protection of almost every asset of every kind, from every adversary type and every general attack scenario.

The true measure of an effective security program is NOT that there have been no losses. More often than not, no losses means there have been no adversarial "attempts"……yet. The true measure is when a loss was successfully prevented or mitigated - in the event of an actual attack attempt - because of the security program then in place.

ABOUT THE AUTHOR

Michael Minieri started a lifelong career in the security profession in 1974 and is the Principal Security Consultant with Minieri Associates Worldwide Security Consultants. He holds numerous professional credentials including CPP, CST, CCO, CPOI, CFPS, CSM, CET, RAM and more. A leading security magazine called him "*…one of the most prominent people in the industry…*" in an exclusive interview and cover story. Complete information and contact details can be found at www.MinieriAssociates.com