Perimeter Security: Deter, Detect, Delay, and Deny

We've come a long way since the days of castles surrounded by moats with squawking geese for alarms and lifted drawbridges to delay access. However, the principles of perimeter security are much the same: it requires a total response that deters, detects, delays, and denies intruders access to your vital holdings.

Deter

A few generations ago, perimeter security was concerned only with "deterrence." Protecting the perimeter was somewhat of an afterthought. Once the main facility was built, access control and building security installed, the project team might say, "Oh, yeah, we better install a fence."

The fence, of course, is a great deterrent. It can be built as a strong decorative fence with heavy iron or a chain link fence with barbed wire offsets and coiled razor wire. Certainly, if your fence is more formidable than your neighbor's, a trespasser will attack the other location instead of yours.

High-security fences are designed with deterrence in mind. Attractive decorative fences can be built to withstand a 15,000-pound vehicle traveling at 50 miles per hour, with a penetration of only 1 meter. This is the US State Department's K-12 rating. We can also electrify a fence, bury the bottom of it, and put stacks of razor tape on top and along both sides. With the world situation becoming more susceptible to terrorist activity, it has become crucial to be able to deter, as well as detect, at the perimeter.

Detect

Detection is necessary because a person can climb over a fence. Sandia National Laboratories' testing has determined that a highly skilled trespasser could get to the other side of a well-designed fence in about 4 seconds. In a high security application, it is accepted that a trespasser will get through a fence within 4 to 40 seconds, so it becomes very important to convey information that someone *has* gotten over the fence, or is presently attempting to do so. This is where *intrusion detection* enters the picture. Factors such as the "probability of detection" and "time to detect" become important, and satisfying these factors will determine which type of intrusion detection equipment to choose.

> "For many facilities, perimeter security is one of the most important applications to install. It needs to be detailed, with a variety of methods that double-check for intrusion, and must be maintained to be effective," says Roy Bordes, President of the Bordes Group and ASIS Foundation Chairman.

Fortunately, there is great technology available to handle detection. Remember the old Jimmy Cagney movies? Jimmy would be breaking out of prison, with sirens blaring and searchlights illuminated to find him. Lights would shine all over the place, but Jimmy would always manage to duck under the light. Well, now it would be somewhat more difficult. With a fiber optic stretched along the fence, an anomaly such as a bend or twist in the optic, no matter how slight, would show a slight variation in the color of the light (different wavelengths contained in white light reflect at different angles). An optical time domain reflectometer (a type of radar for light) attached to the fiber optic would locate the spot, within about a meter, where the twist or bend took place, and a searchlight could be instantly aimed at that point. If Jimmy were running around the yard, a microwave or infrared detector would pick him up. Sorry Jimmy – we gotcha now!

Besides fiber optics, taut wire is still one of the most efficient systems for detection. Wire is stretched tight, like a guitar string, typically at the offsets atop the fence. These tight wires are attached at the end(s) to sensors. Other systems that can be attached directly to the fence include electro-magnetic devices, which can be capacitive or inductive in nature or even magnetic. This type of system works very well to protect a warehouse and surrounding yard. Many airport fences protecting runways have this type of system installed. Magnetic detectors will usually pick up humans carrying metal—even if it's only fillings in their teeth—and will ignore animals.

In an environment that experiences frequent storms, how can a vibration detection device on the fence work well when we don't want to be presented with *nuisance alarms* every time the wind blows? It is possible to install a meteorological system at the fence that will constantly measure wind speed, temperature, humidity, etc., and compensate for changes in the environment. Some systems have a built-in "weather station". Only a rapid change in the environment would cause an alarm (in some cases, we may *want* to know when a sudden windstorm kicks up).

Other methods of detecting a trespasser can take place before someone touches the fence. Fiber optic or electromagnetic cable can be buried in the ground in front of or behind a fence. In the case of fiber optics, pressure on top of the fiber is generated down into the ground, causes the fiber to bend slightly, and changes the color of the light that continues on from that point. Electromagnetically "ported co-ax cable" can also be used. Commonly referred to as "leaky co-ax," it is a system of coaxial cable that has holes in the ground sheath around the conductor, thereby allowing some radio frequency energy to "leak" out. This leaky RF will form a balloon-like pattern above the ground, height determined by depth/distance of cables and nature of the ground. If a body penetrates this balloon-like cloud, the imbalance in the energy will be transmitted to a receiver via the cable system.

Some perimeters may not have fences, such as a body of water. You can protect an area using microwave beams, light beams, or heat seeking infrared detectors. The light beams can be invisible, and some types of beams can even be digital in nature, encrypted to turn on and off at very rapid and irregular intervals, thereby precluding someone "spoofing" the system with their own light source aimed from the transmitter point over to the receiver. Many detectors use dual technology, a combination of RF and light, or RF and microwave, to prevent false alarms. So, now we have "deter and detect." The next step is to delay, and ideally we want our delay to equal at least our response time to deny a trespasser entry to our critical infrastructure.

Delay / Respond

The look and nature of our perimeter security is the deterrent. The technology we have in front of our perimeter and connected to the perimeter will handle the detection. The delay is a function of how long we need to respond. The response can be instant – turning on the lights, sounding a siren, or aiming a video camera along the perimeter to the point of intrusion. A longer response time is required if personnel must rush to the area. In that case, we may have to design layers of perimeter security such as an outer fence with barbed wire offsets, then bundles of coiled razor wire, and inner fencing. Typically, a designer will aim for a 40 second delay at the perimeter by using a series of devices.

Yet, we can have the best detection system available in the world, but if we can't communicate the information that our fence has been breached in a timely manner, the system is worthless. All of the detection and delay technology must have the ability to "talk" to each other, or at least communicate via a software application package of some sort. In the past, every system had its own output that would be wired to a monitoring location. These monitoring locations rapidly became crowded with tens or even hundreds of devices that each had their own operating system and alarm mechanism. The poor security guard had to have an eye on 30 different systems at the same time, and worse yet, had to know how to operate each one using the correct proprietary communication codes.

Now, thanks to modern telecommunications, all the devices discussed here can be combined into one system via the use of TCP/IP, Telecommunications Protocol/Internet Protocol. We can give each sensor in our intrusion detection system, such as the device that picks up vibration at the fence, its own IP address.. This allows two-way communication to the sensor via our computer network, whether it is local (LAN) or remote via the Internet (WAN). This means that the operator can make adjustments *to* the sensor from the control location, or can be notified about something *from* the sensor. All this capability can be integrated into *one* operating system. That system can perform all necessary security functions for the enterprise – functions such as creating badges, keeping employee files, saving monitoring logs of employees coming and going, viewing closed circuit TV, and of course, running the *intrusion detection system.*

With this integrated capability, a fence breaching will instantly show up on a computer screen at the monitoring station, and a response can immediately take place. Since we are using IP addresses, the trespass action can even be sent to someone's PDA such as a Palm or Blackberry! The response can take the form of activating a camera and

allowing the security guard to control it with a pan, tilt, and zoom control (PTZ), or turning on floodlights, sending out a vehicle with guards, activating a siren, or whatever is the appropriate response for a particular facility.

Perimeter security measures are now so sophisticated, that we can set up an "intelligent" video system which will look for certain "situations" needing a response. We can program the intelligent video to alarm if someone is walking in the wrong direction, or if someone starts climbing the fence, or if someone drops a bag and it remains stationary for a certain period of time. Delaying an intruder easy access to the perimeter of our facility long enough to deny him access to our critical infrastructure is the key.

Deny

Finally, you ask, "why is the perimeter so important, anyway? If we have good security at the door to the building, we can keep people out. All we need at the perimeter is a boundary line and a gate." The answer is that people with intention to harm only have to get next to the building to cause severe damage. Remember the Oklahoma City bombing. The perpetrator(s) never even had to leave the curb.

> "The importance of these concepts, **deter, detect, delay and deny** are clearly demonstrated through recently mandated changes in the physical security of the US' commercial nuclear industry," says Haim Perry, VP of Technology for Safeguards Technology, Inc. "Immediately following the attacks of September 11, 2001, the NRC (US Nuclear Regulatory Commission) issued a series of Advisories to its major licensed facilities.
>
> These statements advised licensees to go to the highest level of security, and to further augment their security via increased patrols, additional security forces and capabilities, installation of extra physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls. As the result of implementing the concepts of deter, detect, delay and deny, the security of the nuclear industry has been significantly enhanced."

Even if physical damage to a structure or facility is not an intruder's intent, vital data must also be protected and trespassers denied access to critical information. When you add a total system solution of perimeter security to any building or facility already secured by modern access controls, you create a modern "moat" that protects and secures your infrastructure, denying and controlling admittance to your grounds on your terms.