CPTED Strategies to Maximize the Security of Critical Infrastructure

How can CPTED strategies lead to better physical enterprise security?

A design concept intended to make intruders easily observable, natural surveillance is promoted by features that maximise visibility of people parking areas and entrances. Examples are doors and windows that look onto streets and parking areas, pedestrian friendly side walks on streets, front porches and night-time lighting.

In Rio de Janeiro, Brazil, there has been a long-standing crime problem. However, the neighbourhood of Asa Branca is succeeding in maintaining a peaceful community, free of police interventions. The community has come together to create a community using Crime Prevention Through Environmental Design (CPTED). Thus far, the program, championed by community members themselves, has been a success in an otherwise risky environment.

CPTED brings together law enforcement, architects, city planners, landscape and interior designers and residents to create a climate of safety in a community. This climate is built from the outset of a property or community. It builds security into the infrastructure of the environment and seeks to meld it into landscape.

Richard LeCates is the director of product management, public safety analytics at Central - Square Technologies with offices in Lake Mary, Fla. and High Point, N.C. He says the concept of crime prevention and deterrence as part of design has really been necessary as long as there has been criminal intent. However, he caveats this by saying that where it was once a primary consideration, it is now an afterthought.
“CPTED has been used for a long time. The bollards you walk between on the way in to the bank, pharmacy and convenience store are simple examples of design concepts meant to discourage crime,” he says. “However, the idea of CPTED goes even further back if you consider moats around castles... walls around cities, or even an entire nation – the Great Wall of China [for example].”

Design matters. Careful thought of how and why a facility or a community is designed can affect physical security. He uses school design as an example. School design is driven by budget, seeking to maximize space available for classrooms while minimizing cost. Too much attention to cost constraint may leave security risk unaddressed.

“What has been created is an environment with all the design elements that benefit a would-be perpetrator intending to do harm and doesn’t benefit the would-be victims [or] targets in any way,” he says. Classrooms may have only one access and egress long hallways, which can help armed assailants by prohibiting students and faculty from escaping the threat.

“The design also adds to the chaos and confusion of those fleeing, congregates targets for the assailant and inhibits public safety response and opportunity to neutralize the active threat,” he adds. “This lack of consideration for worst-case-scenarios isn’t limited to just public schools. This is also prevalent in higher education campuses, entertainment venues, etc. Just imagine the last time you left a sport or concert venue and the amount of congestion and extremely limited egress options. The criteria of cost have forced inhibitive design security down the list of priorities, if it is even considered at all. Artificial intelligence (AI) is re-designing structures and we are seeing results that are much more organic, yet use no more materials, improve the pedestrian flow and reduce both the number of collisions and time spent navigating. In addition, safety considerations are made such as minimizing fire escape, or any escape paths."

**Centered on Technology**

A property or community may not be adequately resourced to include the necessary measures, but new communities must give full consideration to the benefit of security technology.

Ken Mills is the chief technology officer (CTO) at Dell EMC, for surveillance and reconnaissance applications. He says the application of technology to design is making inroads. Its incorporation is a boon to CPTED. In such communities, it can do so many things to improve the security of the community. Including it as part of the infrastructure can adequately deter crime and may consequently save lives.

“Less obtrusive camera systems that are gathering multiple types of data, such as audio, infrared and thermographic are now more widely available,” says Mills. “Coupled with better performance in low light and other adverse conditions, and ever-increasing resolutions, we now have a more effective view for what is happening in a given area. Cameras are also getting a lot smarter in that they do more on-board processing, thus pushing insights at the edge.”

Mills adds that the adoption and implementation of the Internet of Things (IoT) means more devices are being installed throughout properties and communities. Such devices provide volumes of data: times of entry, photo frames, log entries and more. This data is information that if used strategically, provides a capability to keep surveillance on a wide area of a community. They provide smart lighting, detect smart phone activity and identify people who are in areas they should not be at certain times of the day. Collectively, this data provides analytics and can enhance a community’s safety. The horsepower of IoT can be instrumental in CPTED in building a secure fortress that can be monitored with visibility and control.

“An important factor in making this all work is to have these smart devices feed into a common shared infrastructure, one that embraces an edge-to-core-to-cloud architecture,” says Mills. “We are seeing more regional agencies do technology planning as a team versus the siloed approach of the past. By
integrating in a cloud component, they can utilize data being gathered by the business community, as well as private citizens.”

As an example, Mills cites the evolution of smart home technology such as smart doorbells and home camera systems that may be combined with the infrastructure laid down by public agencies and cities to provide the widest surveillance and data network in keeping a community safe. “This data being evaluated on a more proactive approach helps law enforcement and the community work together to prevent potential issues by identifying threats before they become a problem,” he says.

**Early Involvement**

Herb Brychta, PSP, CISSP is a physical security risk manager and the manager of security risk management for the design firm AE Works in State College, Pa. Brychta says that too often, security only gets involved with a project after the architects are done and the engineers are wrapping up the utilities.

“At this point, there is no way anyone is going to move a wall because security says it is better CPTED practice to do so – it will simply cost too much as the architects and engineers would have to change all their plans,” he says. “At this late phase, you will be limited to cameras and alarms placement and perhaps moving some lights.”

Brychta emphasizes the importance for security managers to get involved at the inception of a project and make recommendations while the project is still being developed. “Earlier in development, changes are less costly,” he says. “Suggestions to the design can be incorporated to better support natural access control and shape natural surveillance. During early design, I recommend that security managers [and other] professionals analyze how people will flow throughout a space and where people are working. This is a critical opportunity to embed enclaving into a space in a way that makes sense and keeps secure utility areas and back of house functions away from normal building traffic.”

Jeffrey G. Landtiser, AIA, senior project manager and senior claims manager with the consulting firm Rider Levett Bucknall in Phoenix, Ariz. emphasizes the importance of education and awareness when it comes to promoting the overall value of CPTED. “Stakeholders are often surprised to learn that integrating CPTED into a community does not have to be expensive or add cost. Whether part of a new construction project or retrofitted into an existing building or site, CPTED’s intuitive design strategies for access control, surveillance, maintenance and target-hardening can be effective while staying on budget,” he says.

Nevertheless, Landtiser smartly points out that investment in a community by incorporating the complexities of networks, technology and other components has a return on investment that is often tacit, and sometimes over looked. He says, “Making good CPTED decisions doesn’t cost any more than making conventional bad decisions.”