

## The Target Hardening Trap

Tom McKay

---

As a Crime Prevention Through Environmental Design (CPTED) specialist with Peel Regional Police, I am regularly exposed to people experiencing serious security problems. While most of these problems are manageable, no amount of CPTED information will satisfy a person caught in the "target hardening trap".

The target hardening trap is a term that I use to describe a stubborn condition that afflicts some people. The condition begins when an innocent and untrained victim reacts to a criminal threat by responding to a past event. Lacking information, the victim erroneously decides to develop a security response by drawing on his own experience. As this approach is invariably limited, the victim relies on his most recent experience to dictate the first response.

Seldom inspired, the victim adopts a sort of "do-it-yourself" attitude towards security that fails to address the bigger picture or even anticipate the next criminal event. Doomed to failure, the approach quickly takes on a "fool me once, shame on you, fool me twice, shame on me" quality as soon as the next loss occurs. Now more determined than ever, the victim fixates on the latest breach of security to dictate the next response. With the perspective narrowing, the victim becomes more interested in prevailing against a specific kind of previous attack than preventing the next occurrence. The victim has now descended into the target-hardening trap.

I first experienced this phenomena five years ago, when I spoke with the manager of a break-in plagued music store in Brampton, Ontario, Canada. The manager, in response to those break-ins, converted a former single family residence into an extremely target hardened environment. This most notably resulted in two sets of bars on all exterior windows, one set you had to pull out the other you had to push in, a metal grate over the rear entrance door and a steel stockade bolstering the steel front entrance.

Of somewhat lesser consequence was the introduction of an unmonitored alarm, a bricked over milk chute and an overzealous guard dog, which had to be let go for chewing through the building.

Despite these precautions the premise was not safe. In the ten years ending May 1992, the premise had been broken into a total of nine times, the last three happening in a five month period. During two of those attacks, an acetylene torch was used to defeat the rear metal grate and a pick-up truck, possibly a tow truck, was used to pull out the entire rear entrance.

Despite an obvious escalation in the quantity and severity of the attacks, the manager still seemed content to address the problem himself. Fixating on the rear entrances, the manager declared that a steel stockade was needed to protect the already reinforced, metal grated door.

As ridiculous and extreme as this example seems, after-all the manager never did explain how he'd leave the building once the conventionally styled stockades were set, it did happen, and given the manager's reluctance to simply deal with the underlying environmental conditions that made these attacks plausible, i.e. the tolerance of overgrown shrubbery which blocked the view from the surrounding residents, it clearly illustrates what I have come to call the "target hardening trap". This example notwithstanding, it was not until I met another victim reacting in the very same way, that I realized there was more to this story than a good illustration of natural surveillance or the testing of the adage "if they want to get in they'll get in".

The next victim, the owner of a small yet thriving mail machine business, had, after seven break-ins, lost his ability to think objectively about security matters or even accept basic security advice that fell outside of his mindset. Nurtured by multiple computer thefts, the victim had erroneously decided to limit his losses by target hardening the building's interior. Doomed to failure, this approach did little to

address the obvious reasons why the break-ins were happening in the first place. This included the building's remote and screened location and its extensive glass facade.

Instead, the approach resulted in the introduction of a dead-bolt lock to each interior office which apparently did little more than inconvenience the thieves as the break-ins continued to happen. Unperturbed by this setback, the victim fell deeper into the target hardening trap by securing each computer hard-drive with a custom-made, metal jacket that was padlocked to a metal hasp which was bolted to the floor.

Still not safe, the victim only met with police after a perimeter office continued to be entered and the victim was forced to remove the hard-drive to safeguard it overnight. By now, deeply entrenched in the mindset, the victim found it virtually impossible to accept any idea which did not specifically address his latest fixation; the target hardening of the glass.

Not sharing his enthusiasm for this method, I pointed out to the victim that glass break was only one of several methods available to the criminal and in a room such as the one that had sustained the most recent loss, there were two unused, exterior doorways that provided the criminal with the option of a very quick lock-spin or an equally effective frame peel.

As neither of these methods were a concern to the victim, presumably because no criminal had yet demonstrated the likelihood of these attacks, the victim seemed more determined than ever to carry out his plan. Attempting to break through this mindset, I continued to point out the flaws in the plan. These included:

- the prohibitive costs of engaging in such a large perimeter retrofit,
- the need to eliminate redundant doorways to preclude the other forms of attacks, and,
- a general lack of concern for addressing the bigger picture which included the need to address security at the rear of the premise.

Unphased by my comments, the victim's wife effectively summed up our progress to date by stating that they were not concerned about improvements to the rear of the premise as the break-ins never happened there.

With a growing sense of mutual frustration, the victim left me to speak further with his wife after once again asking for a guarantee that they would "never be broken into again".

While extreme in its nature, this example clearly illustrates the dynamics and frustrations of the "target hardening trap". It is the challenge of security professionals and CPTED practitioners alike, to recognize this mindset when it occurs so that we may first develop a dialogue that will allow us to break through this mindset and communicate with these people. Until we assist the victim in escaping the trap, no amount of time, information or good ideas will satisfy the victim.