TrapWire™

General Description

Abraxas Applications

December, 2007

PURPOSE

The purpose of this paper is to advance the concept of TrapWire and training as enhancements to multi-agency counterterrorism programs designed to facilitate the early identification, interdiction and prevention of potential terrorist attacks directed against critical infrastructure and citizens.

BACKGROUND

Most critical infrastructure protection programs today, supported by significant investment, focus on improving perimeter security, access control, and incident response. It is the contention of this paper, however, that we may be able to achieve better results, and do so more cost effectively, by shifting our focus to attack prevention.

The National Counterterrorism Center Report on Terrorist Incidents indicated there were approximately 14,000 terrorist attacks in 2006 resulting in 20,000 deaths in various countries around the world.

KHOBAR TOWERS
(19 killed – 372 wounded)

At the end of FY2007, the Department of Homeland Security, under the Homeland Security Grant Program, had invested approximately $23 billion in local planning, organization, equipment, training, and exercises for state and local governments since 9/11. These grants were intended to "enhance the ability of states, territories, and urban areas to prevent, protect against, respond to and recover from terrorist attacks and other disasters". The vast majority of this money has been spent in support of emergency first responder communities and in defending critical infrastructure by strengthening access and perimeter security measures. Billions more has been invested by the private sector. History has demonstrated, however, that physical security enhancements, while prudent in serving to diminish the affect of an attack, do not prevent attacks from occurring and significant loss of life and critical infrastructure damage still occur. A security audit at Khobar Towers, for example, resulted in the implementation of more than 130 physical security improvements in the months that preceded the attack. Some of the perimeter improvements diminished the impact, but the results were still devastating. There are, of course, many other examples of successful terrorist attacks against "hardened" targets. Additionally, it is difficult to defend "soft" targets such as exist in crowded transit facilities with a physical security enhancement strategy.

The use of suicide bombers and large vehicle-borne explosives provide determined terrorists with significant advantages. Even when facility defenders see these types of attacks coming, as has often been the case, experience has tragically demonstrated that it is then too late to take preventive measures. On the day of the attack, all of the advantage resides with the terrorist. To defeat terrorism, we must intercede when they are most vulnerable – during the pre-attack information gathering and planning process.

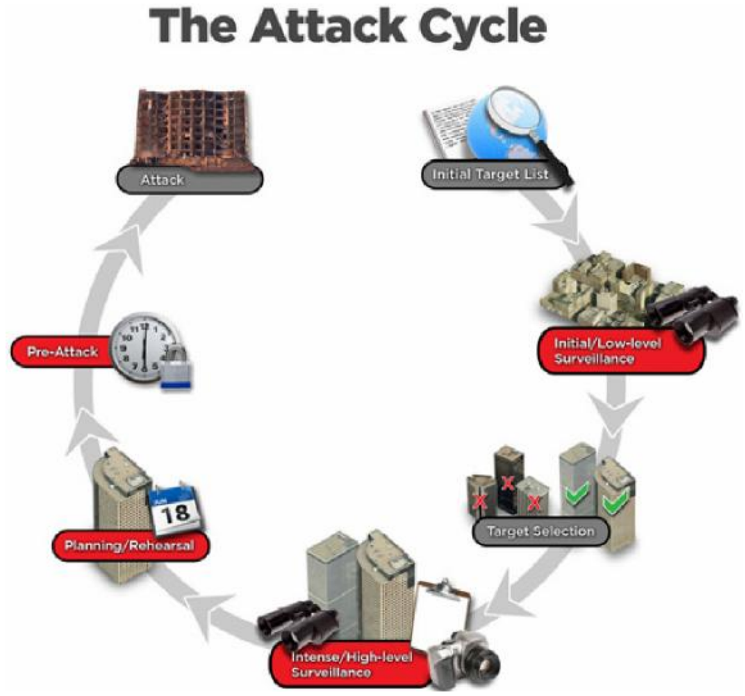
While attack impact mitigation measures are prudent,

attack prevention must be the goal!

TRAPWIRE

TrapWire is a unique, predictive software system designed to detect patterns of pre-attack surveillance. As such, TrapWire represents the basis for a paradigm shift in the methodologies traditionally applied to securing critical infrastructure and personnel; a paradigm shift from the currently accepted and widely adopted philosophy of damage mitigation through increased physical security to a new and proactive approach of attack prevention through the identification and disruption of pre-attack planning and surveillance activities.

While terrorists have developed ingenious methods of attack, and have proven to be extraordinarily patient, every major attack has and will continue to require extensive pre-attack site surveillance. This type of surveillance necessitates multiple site visits over what can be prolonged periods of time. Following the Khobar Towers incident, the Downing Commission report revealed that pre-attack surveillance of the facility was conducted by a three-person team that had visited the barracks on forty (40) occasions over an eighteen (18) to twenty-one (21) month period of time. Employing standard methodology, this same team conducted similar surveillance against other US targets in the region as did Dhiren Barot when he cased and produced detailed dossiers on the Prudential Financial Center in New Jersey, Citigroup Headquarters and the New York Stock Exchange in New York, and the IMF and World Bank facilities in Washington, DC.



A typical Terrorist Attack Cycle is depicted in the illustration. The text highlighted in red represents the periods during which terrorists are most vulnerable to detection. Properly trained security personnel will have the greatest opportunity to detect and disrupt pre-attack planning processes during these periods.

TrapWire was specifically designed to enable security personnel and law enforcement officials to detect patterns of behavior and anomalies indicative of pre-attack surveillance activity and to issue threat warnings in sufficient time to prevent an attack. A unique rules-based engine encapsulates terrorist surveillance methodologies and employs them to analyze suspicious event reports as they are collected over periods of time and across multiple locations. Through the systematic capture of suspicious events and the correlation of those events with activities recorded by public and private facilities across a network, terrorist or criminal surveillance operations can be identified, appropriate law enforcement counter measures employed, and steps taken to apprehend the perpetrators, thereby preventing the attack.

Information sharing and suspicious activity reporting are focused topics of every discussion related to critical infrastructure protection. Yet, today, despite the noteworthy efforts of many agencies, there is no universally agreed upon means of collecting, collating, and disseminating this critically important information. TrapWire addresses this challenge by providing a structured methodology that enables the recording of a suspicious activity in less than 60 seconds. More importantly, TrapWire empowers the leadership responsible for infrastructure protection by providing a means of rapidly querying and analyzing data to identify trends or patterns suggestive of pre-attack surveillance in sufficient time to intercede. To facilitate the sharing of recorded information, TrapWire is unique in that it does not capture, store, or share any sensitive or personally identifiable information.

CONCEPT OF OPERATIONS

SITE SURVEY: Each TrapWire deployment is preceded by an extensive and comprehensive site survey conducted by experts in the areas of terrorist target assessment, information acquisition methodologies, and surveillance techniques.

The purpose of the site survey is to identify:

- Targets of terrorist surveillance;
- Zones from which terrorists are most likely to conduct surveillance;
- Extent of existing facility video systems coverage; and
- Time sensitivities/vulnerabilities.

In the process of conducting pre-attack surveillance, terrorists attempt to avoid detection by seeking surveillance zones that offer lines of site to surveillance targets <u>and</u> adequate cover. The Site Survey will identify the locations, referred to as "Red Zones", which are most likely to be used by terrorists for target information collection; and will determine if these areas are adequately covered by existing video systems.

INTEGRATION: TrapWire is integrated with and utilizes existing surveillance technologies (such as pan-tilt-zoom [PTZ] cameras) and human observation to capture photographic or video evidence of suspicious activity.

TRAINING: Abraxas Applications provides specialized training programs designed to support the TrapWire implementation effort and to improve overall security effectiveness.

Security Awareness Workshop. The four-hour Security Awareness Workshop is taught by individuals with extensive surveillance and intelligence operations experience. The purpose of the Workshop is to:

- Instruct students on the specific objectives and potential targets of criminal or terrorist surveillance cells;
- Sensitize security personnel to surveillance methodologies and the likely use of Red Zones surrounding a facility;
- Advise students as to the importance of focusing some of their attention outside the facility perimeter and of reporting on ALL suspicious activity; and
- Improve upon the Observational Awareness Skills of each student through a series of exercises and lectures.

TrapWire Operations Course. The two hour TrapWire Operations Course is designed to instruct designated security personnel in the operation of the TrapWire system.

CONCLUSION

TrapWire, its related methodologies and global database, has the potential of converting a group of otherwise isolated facilities (and events) into an information collection and dissemination network that can significantly enhance the ability of participating facilities and law enforcement agencies to detect terrorist or criminal surveillance activities and prevent attacks.

CONTACT

Daniel V. Johnson
Senior Account Executive
Direct: 703-462-5838
Cell: 651-245-9962
dan.johnson@abraxasapps.com

R. Dan Botsch
Vice President, Operations
Main: 703-462-5800
Direct: 703-462-5804
dan.botsch@abraxasapps.com

ABRAXAS APPLICATIONS

Abraxas Applications is a technology and services company that leverages its extensive knowledge of terrorist behavior and surveillance operations methodologies to develop and market products and training courses intended to prevent terrorist and other criminal attacks against critical infrastructure, key assets and personnel.