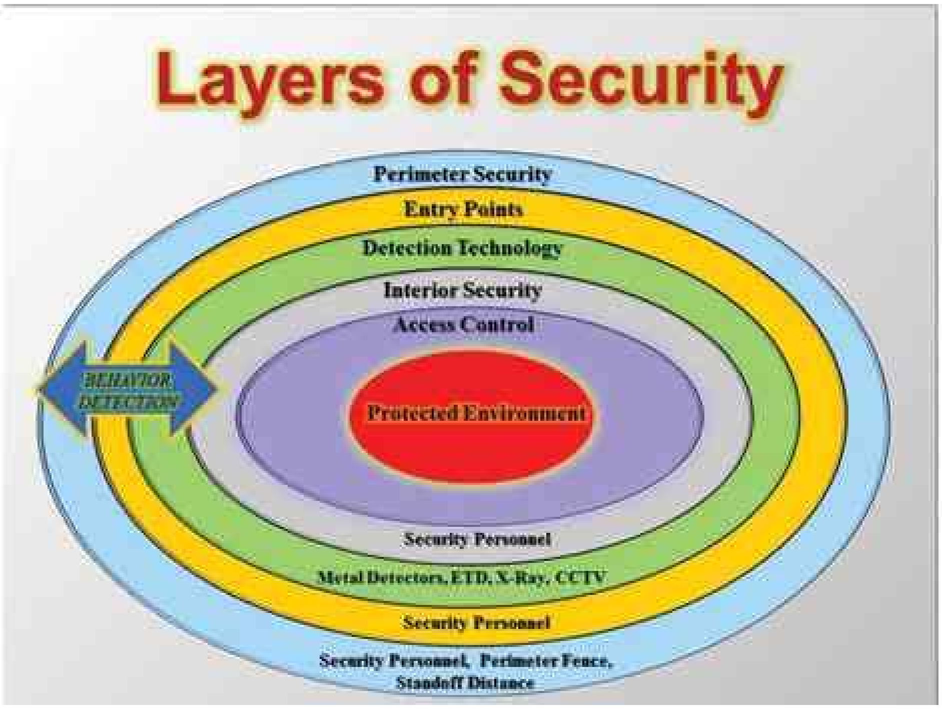
SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

Home

U.S. Security Shifting to Preventative Methods

By Michael Rozin
October 1, 2012



Let’s start with the basics: the reason we take off our shoes at the airport is because the shoe bomber tried to get a bomb on a plane. The reason we can only carry on 3-ounce bottles? Someone tried to get a liquid bomb on a plane. Body scanners? Underwear bomber. But what if we took a look at suspicious behavior of the people attempting these acts of terrorism instead of relying primarily on machines to do our dirty work?

From state law enforcement to federal law enforcement agencies, from in-house security to contract guard force management companies, there is a live and dynamic movement across the United States to re-design existing security strategy, and attempt to incorporate more dynamic, effective and overall proactive security programs. It’s called many names: Behavior Detection, Behavior Pattern Recognition, Security Profiling, Behavior Assessment, Screening of Passengers by Observation Techniques (SPOT), Suspicion Indicators Recognition & Assessment (SIRATM) and many more. But what’s it all about? Let’s start with a real life example.

Guy with a Gun

An officer trained in Behavior Detection in a busy public space sees an individual who acts differently than what would be considered normal for this environment. He's carrying an unusual pouch, seems nervous and attempts to calm himself when a security officer walks nearby. The officer, following his operational protocol, decides to engage by asking a few questions. After two initial questions the interviewee starts to sweat and tries to calm himself. After two more questions the individual decides to take off. He's eventually apprehended and in his belongings, they find a loaded handgun. Then they learn he has a history of violence and belongs to a group associated with targeting specifically this very organization. He states several times that he came to fulfill "his mission" that day. Although his intent would be hard to prove in court, from a security perspective, this is clearly a crime deterred.

Sounds simple, right? Maybe it is. Here's how it breaks down.

The Threat

Everything we do in the security field is threat-centric. When there is a threat, there is a need for security. When there is no threat, there is no need for security. Interestingly enough, if you think holistically about the threat concept – it is the possibility for an occurrence of a relevant hazard we in security are attempting to prevent. By this fact alone, the security operation of any organization, big or small, must be proactive. When a security operation is strictly reactive, the objective of security existence is not being met.

"It is our continuous pursuit of providing more effective protection to our clients that made us look into behavior detection," says Tim Kingsley, Associate Vice President at American Security & Investigations in St. Paul, Minnesota. The company recently went through behavioral detection training to strengthen its client offerings. "No closed circuit TV camera is as effective in protecting our clients' assets as a well-trained security officer capable of identifying harmful intent and asking the right question at the right time," he adds.

So what is threat? Operationally, there are two main factors that create man-made threats: Means (as in weapons) and Intent. Simply put, for the "bad guy" to cause harm he/she needs to have a gun, knife, explosive device, etc., but also have intent to cause the physical harm. A person with access to weapons, but lack of malicious intent is not a threat, nor is the person with malicious intent but with no access to weapons (think inmate). It is only the combination of these two factors, means and intent, which creates the threat.

When you think about past acts of violence, like the World Trade Center bombings, Columbine or the recent shooting in the Aurora, Colorado movie theater, you'll notice they happen at different locations, are conducted by different perpetrators, with different motives, utilizing different weaponry and methods for an attack. The only common element between any and all acts of violence or man-made threats is the intent.

People planning to commit violent acts, consciously or unconsciously, show indicators or "traces" that expose them to possible detection. Traditional methods for attempting to discover aggressors' plans, especially in the U.S., have focused on detecting weapons. Such a focus has often been unsuccessful in detecting and preventing terrorists from executing attacks. I'll list a few examples:

The terrorist attacks on 9-11-2001, Richard Reid aka “the shoe bomber” (12-23-2001) and Umar Farouq Abdulmutallab, otherwise known as “the underwear bomber” (12-25-2009).

One of the major successes of the Israeli security apparatus where I worked for five years was its development and use of methods to identify harmful intentions. Based on its successful use of those methods, the Israeli security agencies determined that harmful intent is often the best method, and sometimes the only practical method, for detecting a planned terrorist attack.

This focus on intent is the key underpinning of the Behavior Detection, which enables trained security personnel to identify behavioral traces, consistent with harmful intentions. This focus, in turn, enables security programs to be more proactive – by identifying pre-incident indicators, thus increasing the ability of security operations to thwart acts of violence targeting their premises.

Effective Security Strategy

Most security operations typically have two general functions: to protect the defined assets and to respond to incidents. But what is protection and how does the Behavior Detection support this most essential security mission?

The following three security objectives define the term protection:

- **Deterrence**– the ability to affect the motivation/psychology of the attacker and direct them to a different target.
- **Detection** – the ability to identify the hazard usually at a portal or defined site (“at the last moment”).
- **Prevention**– physically intercepting the attackers, after the initial sequence/planning of the plot has been carried out.

Over the years, many case studies have showed us that security technology, physical security measures or security personnel alone do not deter the perpetrators of violence. What does deter the aggressors is a security system capable of identifying intent through continuous and unpredictable security measures. When a potential perpetrator is planning his/her act of violence, the two most important elements he/she will consider are: simplicity – how complicated is to obtain the weapon and execute the plot; and ease – how difficult is to access the desired target undetected and execute the planned attack. The security system of any organization is unlikely to have any influence over the simplicity factor. This is because it is out of our control how complex or simple the plot is; what type of weapon they choose; and how they intend to deliver and apply it to cause harm.

We, in security, however do have a direct impact and responsibility on how “easy” our protected environment is perceived. This is precisely where Behavior Detection program has magnificent impact. Behavior detection creates a very dynamic security officer, who is continuously looking for slightest signs of potential threat elements. It allows the security to look for, and identify, malicious intent continuously, unpredictably and effectively. It is not the metal detector, x-ray machine alone that will create an impression of hard to penetrate security, but rather a combination of technology, physical security measures and most importantly well-trained security staff capable of identifying indicators consistent with harmful intent and asking the right question at the right time.

“Now my staff knows not just what to look for, but how to act on it in a professional and systematic manner,” says Kingsley. “No criminal wants attention drawn to them, and simply asking a few good questions can be a strong deterrent.”

Terror in the Skies

Take, for example, the security of El Al airlines.The only successful hijacking of an El Al plane was in 1968 when a flight from Rome was hijacked by members of the militant Popular Front for the Liberation of Palestine (PFLP) and forced to land in Algiers. The desire to carry hijackings and/or bombings on El Al airlines hasn’t diminished. The perpetrators simply don’t try any more.

Fast forward 30 some years for a more current example. Richard Reid – or “the shoe bomber” as you may know him – initially targeted El Al’s flight. Knowing of the sophistication of El Al’s security, Reid was sent by Al-Qaeda to conduct surveillance and learn the security process. When he attempted to board the flight from Amsterdam to Tel-Aviv, he was defined as suspicious, questioned by El Al security and defined as a potential threat. Reid was meticulously searched and seated between two El Al Air Marshalls who breathed down his neck during the entire flight to Tel-Aviv. Once in Ben Gurion Airport, Reid was questioned by Israeli Security Agency (Shin Bet) and then released. When he reached his destination – Al Qaeda camp in Afghanistan, Reid reported: “It is impossible to hijack an El Al flight.” Al Qaeda then chose to carry an attack on American Airlines.

The difference between the security systems at El Al and American Airlines in this example was the focus on intent (El Al Airlines) vs. weapons (American Airlines) and the result was obvious: behavioral detection worked. Richard Reid, and Al Qaeda, chose an easier target. This deterrence effect is one of the best qualities of a behavior detection system. Behavior Detection creates a strong security impression, and shows a potential perpetrator that they can be sniffed out.

What to Look For

What should security agents be watching for? There are several categories of suspicion indicators that take into account potential aggressors’ methods of operation holistically. Let’s focus on one of these categories: behavior and appearance.

The underlining concepts behind these indicators are: a) our body naturally reacts to danger and stressors, and in this case the stressors are security or law enforcement officers and b) aggressors typically attempt to blend into the targeted environment prior to the execution of their planned attacks. Furthermore, the indicators of fear and detection, as result of a stressor, are authentic, produced by a special part of our brains, and cannot be manipulated. What it means is this: when you’re nervous, you act differently than people who are not. You might sweat, walk differently, attempt to blend in and try to calm yourself. You can’t help it. That’s your body’s natural reaction. Those things are visible to others.

Conversely, someone simply shopping in a mall or trying to get on a flight doesn’t act suspiciously. They don’t react to a presence of security/ law enforcement or change their pattern of walking. They aren’t a threat.

But suspicious doesn’t mean guilty, so what do you do about it? You ask questions.

Security Interviewing is an effective method of asking questions in a polite, professional and systematic manner. The answers along with interviewee’s nonverbal response to our questions allow us to corroborate information and determine whether there is a threat. At this point, security personnel may have already prevented an act of violence.

Implementation of Behavior Detection Program

The following is the typical process of developing and implementing a behavior detection program:

1. Risk Assessment
2. Operational Protocols & Policies Creation
3. Personnel Selection & Training
4. Red Teaming
5. Continuous Evaluation

1. Risk Assessment

This is the foundation of any security program. Take a holistic look at your organization’s relevant aggressors’ potential methods of action, existing security technology, physical security measures, operational protocols, staffing and personnel deployment.

2. Operational Protocols & Policies Creation

A well-conducted risk assessment will identify most likely aggressors’ potential methods of action, define the typical legitimate profile at one operational environment, and suggest operational deployment of behavior detection trained assets to counter the identified risks. All these pieces of information derived from the risk assessment are necessary building blocks of any Behavior Detection program.

Risk assessment is followed by the creation of operational protocols to address Security Interviewing, immediate versus non-immediate threats, deployment and more.

3. Personnel Selection & Training

Not everyone has the right combination of experience, personal skillset, charisma and determination to conduct effective security interviews. Therefore, selecting proper personnel for this type of work is essential.

Training is the natural next step for implementation of Behavior Detection programs. Typical and effective Behavior Detection training must incorporate in-class and field training and exercises. On average, five days of training is the minimum necessary time needed for security professionals to understand, internalize and have basic experience applying the system on the field.

4. Red Teaming

Red Teaming is about accountability. It ensures continuous top performance of trained human assets on the field. It is authorized assessment, performed from an adversary standpoint, to ensure your organization’s capability to detect and prevent aggressors’ potential methods of action.

5. Continuous Evaluation

It’s critical to have an open and flexible system to account for changes driven by Intelligence Information, field analysis and Red Teams. Therefore, an ongoing evaluation must be sustained of the program to ensure the program is vibrant and capable of meeting its objectives of deterring, detecting and preventing potential threats.

Creating a More Dynamic Security Team

In addition to operational effectiveness, Behavior Detection programs help create a more dynamic, professional and motivated security team. It is the core mission of any security entity to protect. Behavior Detection, in combination with security technology and physical security measures, allows for an effective protection program.

This article was previously published in the print magazine as "Security in the States Shifts Focus to Prevention."

Michael Rozin is president of Rozin Security Consulting, LLC. His background includes Special Operations Security Captain at the Mall of America, where he developed, implemented and managed a behavior detection unit and a variety of additional innovative security programs focused on mitigating the threat of terrorism. He is a regular guest speaker at law enforcement and security conferences on counter-terrorism, suicide terrorism and proactive security methods. He has trained a number of law enforcement and security agencies on counter-terrorism and tactical response techniques. He is also a certified law-enforcement and civilian instructor in Krav Maga defensive tactics and fluent in Russian, Bulgarian, Hebrew and English.