

# ***BEFORE TERRORISM STRIKES***

## **THE AGGRESSION MANAGEMENT® IDENTIFICATION SYSTEM**

I recently read in *Risk Management Magazine* the Jared Wade article “When Suicide Bombers Attack.” *When* they attack? Isn’t that too late? We are told to look for a “smoking gun”. But smoke means the bullet has already been discharged. Isn’t that too late? Now that we know that terrorists are prepared to give up their lives for a cause, to drive a truck or an airliner into a building and detonate it without regard for their own lives, we must seek solutions that deal with those precious, fleeting hours and moments *before* suicide bombers attack.

We are now engaged in what has rightly been called the “War on Terrorism.” And no war has ever been won by great defense, by hunkering down and waiting for the enemy to attack, or even more to the point, by using vague, inexact methods to identify that enemy.

For that reason, Aon Corporation’s Aggression Management® Identification System (AMIS) has been developed to be an effective, proactive terrorist detection system. It employs a proven continuum of cognitive human behavior that identifies a probable terrorist using quantitative, measurable Aggression Management methodology.

One way to define AMIS is to delineate it from currently used terrorist identification methods. After the shock of 9-11, law enforcement and security professionals rushed to establish means of identifying a terrorist in crowd of travelers. Civil libertarians rushed alongside them, seeking to preserve the rights of citizens who might be caught up in the net of suspects and “persons of interest,” based on a variety of criteria. Let’s examine a few of the systems created to preclude an act of terrorism, examples of what AMIS is *not*.

### **HARDENING THE TARGET**

Terrorism is a threat that could emerge from anywhere and at any time. However, it can be prevented if you know what to look for. Most organizations are attempting to “harden the target” through expensive electronic physical security measures. Yet the question is, can you build an electronic physical security system beyond the capability of determined, ingenious terrorists to penetrate that security?

I recall a government IT department that went to great lengths and expense to harden the entire fifth floor of a county office building. There was absolutely no way to enter this floor without the express permission of the receptionist. She was a trusted member of the staff; however, she had an abusive husband who swore that she was having an affair with one of her co-workers. In order to stop her husband’s badgering and quite his fears, she allowed him access.

The Orlando Sentinel reported “undercover agents arrested six people August 21, including five current or former baggage handlers on charges of sneaking drugs or guns past Transportation Security Administration screeners onto flights”. At the beginning and end of every security system is a human being, who through human frailty, greed or malicious intent can destroy your considerable investment in security.

And there is the story of Michael McDermott, 42, who came to his workplace – Edgewater Technology, a computer based organization – and shot and killed seven co-workers before he

was subdued. As a high tech organization, Michael's employer had one of the most sophisticated security systems available. In the first news article after Michael's carnage, his company stated, "There was no way to anticipate his actions or any apparent reasons to restrict his access to the building". Then, finally, there is the reality that many organizations face, that it would be exorbitantly expensive to secure their facilities and it's simply too impractical to consider.

Within the realistic budget of a corporation, Even the most sophisticated electronic security system cannot alone cannot sufficiently defy the genius, the determination or overcome the frailties of the humans without additional human training.

### **STEREOTYPE PROFILING**

Some organizations choose to use profiling methods to identify a potential terrorist, but profiling can only tell you that, within a certain group of individuals, there is a higher probability of a terrorist presence. It cannot tell you *which* individual will be your next terrorist. The only way to make profiling more effective is to make it more invasive. The CAPS II (profiling) program used in airports fell into disfavor because the next step to effectiveness was to collect private home addresses and phone numbers of airline passengers. Civil libertarians protested and Tom Ridge, head of the Department of Homeland Security, scrapped the program.

In addition, we know that criminals and terrorists sometimes do their homework. One of the terrorists on 9/11 bought his tickets months before the event, wanted roundtrip tickets and frequent flyer miles! This, of course, took him outside the profile. While the flying public scoffs at a security system that shakes down old ladies, children and Norwegians, it is important to remember that all a terrorist needs to do to beat profiling is to *not look like a terrorist*. At the same time, such a system only achieves political correctness and underscores the need for a more sophisticated, quantifiable means of detection.

Furthermore, profiling as a method of identifying a potential shooter was denounced by a joint study conducted by the U.S. Secret Service and the U.S. Department of Education in their report on *Targeted Violence in Schools*. It suggested, "An inquiry should focus instead on a student's behaviors and communications to determine if the student appears to be planning or preparing for an attack."

That in fact is the basis for AMIS - the use of behavior, body language and communication as indicators to measure emerging aggression.

### **BODY LANGUAGE PROFILING**

Others are using body language profilers to identify a terrorist. A *Wall Street Journal* article explains how Boston's Logan Airport trained 200 Massachusetts state troopers to watch for things such as darting eyes and hand tremors and to conduct rapid-fire questioning to find inconsistent stories. "Terrorists behave differently than legitimate passengers", says Rafi Ron, an Israeli security consultant, who contends "well-trained body-language profilers might have spotted and questioned some of the September 11<sup>th</sup> hijackers by very basic behavior pattern recognition work".

Outside the usual questions of stereotyping, the *Wall Street Journal* article goes on to quote David Harris a law professor at the University of Toledo College of Law, who is extremely concerned that the use of profiling 'raises the specter of anxious travelers coming under

suspicion when they are just nervous about flying'. The concerns of Harris and other civil libertarians can be substantially alleviated by measuring emerging aggression through the use of the AMIS.

Although body language profilers do use behavior and body language to some degree, AMIS provides a proven method that is very different. First, the behavior indicators we identify are different, which enable us to separate the nervous passenger from those with fatal intentions. Second, we *measure* these elements to enable an interviewer the ability to size up a ticket-holder for indicators of terrorism. The important question becomes: "Do I allow this person on that plane?" If you can't measure aggression, you can't answer that question. Consider the incident with Richard Reed, the shoe bomber. Security professionals kept Reed from boarding the plane because their "gut instinct" or intuition told them that Reed was a problem. They were reading his body language, behavior and communication indicators. But because they were unable to measure his aggression, i.e., his potential to be a suicide bomber, they had no sound basis to keep him from boarding the plane the next day.

### **INTUITION OR "GUT INSTINCT"**

Still other security organizations are using "gut instinct" to identify a potential terrorist. This becomes clear when *New York Post* reported that "New York police officers are to be on the lookout for men *who appear freshly shaven with cuts or nicks* -- which could indicate a beard has just been removed -- as well as anyone with ill-fitting uniforms or unfamiliar forms of identification." Although both proactive and imaginative, it was obvious that NYPD need more formalize and measurable method of terrorist identification.

Without a reliable measurement tool, most security officials are forced to rely on observations and intuition to identify and prevent terrorist activity. Most of these officials are not prepared to put their reputation - and their jobs - on the line based upon intuition. Consequently, nothing is done; suspicious activity is not reported, and "after the fact" security people stand around saying to each other, "I knew that guy was like that". One organization explained that out of their 50 security personnel, only eight were incredibly intuitive, and would take action based on their intuition. The remaining 42 would not. They needed an objective system that would support their taking immediate action, one that provides scientific validation and legal justification for identifying and detaining a potential terrorist suspect. AMIS is such a system.

### **CAN WE MEASURE THE AGGRESSION OF A TERRORIST?**

Ten years ago, there was only "aggression." As I studied this elusive topic, I realized that there were actually two types of aggression: Primal Aggression™ and Cognitive Aggression™. For each form of aggression we have created a Continuum- a method of measuring each based on behavioral identifiers. Primal Aggression™ is based upon the primal instinct of fight or flight, fueled by adrenaline and indicative of someone losing control and attacking their victim.

But what about deliberate, premeditated aggression? I call this Cognitive Aggression™, driven by a cause or intent, and indicative of a victimizer, a predator and a *terrorist*.

Typically, as he or she moves toward an act of aggression, the behavior of an aggressor climbs both the Primal Aggression Continuum™ and the Cognitive Aggression Continuum™ concurrently. A potential terrorist, however, can move up the Cognitive Aggression Continuum and not yet be in the presence of a victim. Although we focus here on terrorism, this could represent *any individual who is prepared to give up his or her life for a cause*.

We've heard that terrorists "find a profound calm" before they carry out their violence. This is because they have completely detached themselves from their own well-being. This causes the aggressor to exhibit certain behavior, body language, and verbal communication indicators that can be identified and measured – which is how we distinguish a terrorist from a person who is simply afraid of flying, a concern of civil libertarians.

Furthermore, much like cutting off oxygen, it doesn't matter what culture, gender, age or education they are, humans will all respond similarly. These Aggression Continuums will make it easier for an observer to measure a potential terrorist's indicators for aggression while avoiding the civil liberties quagmire of appearance, ethnicity, age or gender.

AMIS provides a quantitative measurement of emerging human aggression. It uses a synthesis of data, based on the research of a list of eminent scholars in human behavior. The Cognitive Aggression Continuum enables a security official to observe and measure the emergence of aggression in any individual. It works whether the suicide bomber is an old lady, a child or even of Norwegians heritage.

#### **IF YOU CAN MEASURE IT, YOU CAN MANAGE IT**

A tenet of Total Quality Management states, "If you can measure it, you can manage it". This principle can be used to evaluate the productivity of an office, an assembly line, a school district or an individual employee. Risk managers, safety engineers, security managers and human resource directors use these performance measurement systems to convince superiors of the effectiveness of quality initiatives. Aggression is no different. If you can measure aggression in others - and yourself - you can manage aggression in others - and yourself.

In today's litigious environment law enforcement officers find themselves more frequently in front of a judge explaining that they engaged a subject because of their 18 years of police experience and their "gut instinct" or intuition. Judges and magistrates have previously permitted this kind of engagement. Nowadays, however, under the intense scrutiny of civil libertarians, intuition is not enough. AMIS makes this process more objective, enabling law enforcement and security professionals to ultimately achieve what their greatest objective, we often call the "holy grail", – legal defensibility.

In a world where reacting to terrorism is not good enough, we need a **human technology** that permits us to identify the next suicide bomber *before* he strikes.

The Aggression Management Identification System enables us to accomplish this.

###