The shoe bomber, the underwear bomber, bombs in computers, bombs in cell phones, and the list goes on, for those who are aware of the actual threats aviation has faced. Explosives have become the 21st century threat to aviation and other critical resources, overcoming guns and knives, the tool of a past generation of terrorists and hijackers. And the ease with which these threats can be deployed has increased the cost to the industries that need to protect against them.

But the security industry has responded in kind, developing technologies that can detect anomalies and provide the indicators needed to identify a potential explosive device in people and packages entering a secure area. And of course, these technologies come with the protocols to follow to use their inherent clues to thwart the threat.

So why do oversight organizations, from the Department of Homeland Security Inspector General to Australian authorities, continue to see performance problems? Why is the technology and the processes to apply them, seemingly with the ability to detect the problem, not sufficient to keep our critical infrastructure safe?

The answer lies in the fact that true security effectiveness is achieved by a blend of technology, process, and human interpretation. And the human factor is probably the most important, and the most difficult to get right. People are the variable that changes, that understandably have variations of interpretation. Misinterpretation, unfortunately. Making the human assessment more consistent with what the technology is indicating, is the goal.

The reality is that human interpretation of any indicator is subjective, it's dependent on the state of mind of the person responsible for determining if what they see is sufficient to require further scrutiny. It's about training, fatigue, complacency, commitment to mission, and an understanding of the limitations of technology. All of the human factors that may lead to variations in a critical security decision.

The right decision, when enough of the indicators are there, is to move a suspect person or package on for further screening. And when that happens, the chances of finding that one in a thousand possible threat increases exponentially.

So how do security executives determine if their workforce has a common mindset, a good understanding of the tools they are using and procedures they are deploying, to make the right call when so much is at stake? It's through covert testing, the same process used to demonstrate deficiencies, but with enough testing to show where improvements are needed.

Covert testing provides a true measure of the effectiveness of a security program. But unlike many of the tests conducted by oversight agencies, a mature covert testing program provides sufficient testing to make a data supported decision regarding the weaknesses of that program.

Oversight agencies often run a few tests, find they can sometimes defeat a security measure, and demand improvement. And while this can be enlightening, and shines a bright, and unfortunately dangerous light, on the security system that is under review, it stops short of developing enough information to be useful.

It's this same technique, if applied multiple times in a systematic, consistent manner, that can provide decision makers with an understanding of why the system is failing. Questioning those who did not 'find the bomb' in a non-threatening way and analyzing patterns that were common among a variety of

screeners, helps to uncover root cause. It helps to explain why our initial assumptions regarding a security system, that seemed effective on paper', failed too often.

Two comments on the data collected, which will be discussed in future posts. The first is that the information uncovered, especially in its totality, must be protected like the Crown Jewels. As important as this information is for security professional looking to close gaps, it's equally valuable to an adversary looking to exploit those gaps.

And the data collected is only worthwhile if the analysis and the corrective measures It suggests are given serious consideration by decision makers. Too often the scrutiny that reveals flaws does not reach those who have the authority to bring about change. Covert testing needs the backing of security executives, or its results often provide no more than a 'wish list' for those on the ground, striving for improvement.

And the improvements are not typically costly. Often, it's as simple as tweaking the existing training program, or making subtle changes in procedure, that will bring about positive change. No security system is infallible, but every system can and needs to be constantly evaluated for improvement. And covert testing is one of the most effective ways of revealing what changes are most needed.