The Underwear Bomber

A Case Study of Inside-Out Risk Management

Kip Hawley
Center for Homeland Defense and Security
Dept. of National Security Affairs
Naval Postgraduate School

Slide 1

Opening Credits

Music

Slide 2

The Underwear Bomber: A Case Study of Inside-Out Risk Management

By Kip Hawley

Slide 3

Case Study: The Underwear Bomber

The Case of the Underwear Bomber, Umar Farouk Abdulmutallab's failed attempt to blow up a passenger plane on Christmas Day, 2009, is chiefly remembered as a shocking demonstration of the aviation system's vulnerability. Eight years and billions of dollars after 9/11, a single man was able to defeat security and bring a bomb onto a commercial airliner, very nearly destroying it and killing 300 innocent travelers. It appears that the primary lessons learned are that we have to improve our intelligence coordination and upgrade security technology at airport checkpoints. I suggest that there is another lesson to be learned: that the Underwear Bomber is a case study of what I call, "Inside-Out" risk management.

We all talk about "risk management" in Homeland Security issues, but sometimes it is difficult to grasp how it specifically applies to on-the-ground problems. Inside-Out is one way to think about risk management, essentially looking backwards along the critical path from the event we want to prevent.

Rather than look at it "Outside-In"—starting from where you are and working towards the danger you are trying to avoid—you instead reverse-engineer backwards from the worst-case scenario, trying to take away critical elements that might expose new ways of defeating security.

Just as al-Qa'ida exploited our cultural norms by concealing its bomb in the core of a person's private parts, we can use Inside-Out thinking to protect the transportation system from catastrophic attack. Here is the case study.

Slide 4

Christmas Day 2009

The Christmas quiet was suddenly shocked into a news frenzy when Northwest Flight 253 landed in Detroit from Amsterdam. A man was taken into custody and the buzz emerged that there had quite possibly been an attempt to detonate a bomb during the flight's approach into Detroit. For several days, there was blanket coverage by all forms of media as authorities, reporters and citizens sought to understand what had happened and prevent further damage. Who did it? Was it an organized attempt? Are there other attempts in progress? How did he defeat security? Why didn't we stop him? Is security in other countries up to the job? How serious is this problem? What can we learn to strengthen the system? The first question in the minds of those within Washington's Capitol Beltway hung like a dark looming cloud, mostly unspoken, over the whole matter – 'who is to blame?' First, let's take a look at what happened.

Slide 5

Defeating Checkpoints

As with any real world event, multiple dimensions are in play and the only fair summation is that the situation was complicated. A closer look at the specific physical security measures, however, gives us some surprising insights. This case study will focus on checkpoint security procedures to isolate a key, but not obvious, concept in transportation security risk management.

Let's establish that Abdulmutallab was trained by al-Qa'ida and moved into position where he would gain access to his intended target, Northwest Flight 253, a packed Airbus 330 heading to Detroit. He was clever about his flight bookings and cross-border requirements. Unlike Richard Reid in 2001, he did a good job playing the part of a buttoned-up, pleasant young man so that authorities would not pick up on any behavioral cues or play into racial or cultural bias. So, on December 24/25, Abdulmutallab presented himself – fully kitted out with a powerful PETN-based bomb – at security checkpoints in Lagos, Nigeria and Amsterdam, the Netherlands – and went right through.

How did that happen?

Slide 6

Security by the Book

First, this was not a case of bumbling security operations at either checkpoint. Security officers examined his carry-on and his shoes. Adbulmutallab was checked for liquids in containers large enough to hold sufficient explosives to destroy the aircraft and was clean on all counts. He did not alarm either magnetometer and even got a light pat-down at Schiphol in Amsterdam. He was also interviewed briefly while his documents were examined and he exhibited no objective or subjective signs that anything was amiss.

Though security procedures were executed by the book, they did not stop the bomber. It is interesting to note that all the technology needed to detect the bomb was at Schiphol that morning. The body scanners were in another pier but explosives trace detection equipment was right there when Abdulmutallab went through. In this case, "by the book" also meant that he did not qualify for that extra test, so he would have known that if he didn't trigger an alert based on the previous security screens, he could get through without a problem. Only watch-listed passengers or those with suspicious objects were sent for the explosives residue testing.

"By the book" security is an example of one of the weaknesses of Outside-In security. Harmful objects are identified as prohibited, written down in TSA requirements, and taken away if found. Based on experience and intelligence, Outside-In security tries to account for the scenarios considered most likely.

Slide 7

In Position: Taking a Seat

Once through security at Schiphol Airport in Amsterdam, Abdulmutallab settled himself on Northwest Flight 253 in his carefully selected seat, 19A.

Just like Richard Reid during his shoe bomb plot in 2001, Abdulmutallab was positioned perfectly—next to a window and directly over the fuel tank. Hours later, with Flight 253 over the North Atlantic, an analyst at Customs & Border Protection at its National Targeting Center would piece together that Abdulmutallab was a problem and arrange for him to be met on arrival in Detroit. But by that time it would be too late.

Abdulmutallab was two for two in penetrating mainstream aviation security right through the front door and found himself airborne in this selected seat on fully loaded Flight 253. Next stop, immortality.

But despite al-Qa'ida's success in placing their agent with his artfully concealed bomb components, the plot was unsuccessful and Flight 253 landed safely in Detroit.

Why?

Clearly there were security failures throughout Abdulmutallab's mission. Despite them all, other aspects of the aviation security system held together and saved the day. Let's take a closer look.

Slide 8

How Do You Blow Up an Airplane?

Contrary to what you might think, commercial airliners are hard to blow up. Airframes are extremely resilient and have gotten progressively stronger as better materials and assembly techniques, as well as more demanding safety requirements, are introduced. For instance, passenger aircraft are required to be able to land on a runway (or water) without wheels – meaning

they come in heavy and hard and scrape their way down the runway until they stop, when the emergency slides deploy and the passengers and crew exit to awaiting CNN reporters.

The Hudson landing two years ago is a memorable example; however, landings without wheels, or sometimes landing with large holes in the fuselage, are not rare.

One extreme example of this is Aloha Flight 243, which, in 1988, lost its entire roof and landed safely, resulting in only one fatality.

Even at pressurized altitude, blowing a hole in the fuselage does not necessarily bring a plane down. So what does? We will look at several dimensions of this question.

Slide 9

Placement Matters

The first is placement, which matters a great deal. Where is the bomb in the airplane when it explodes?

There is a relationship between how close the bomb is to the skin of the aircraft and how big a bomb you need. A bomb of "X" size blowing up in the center of the aircraft has its effects attenuated by the distance and the tamping effect of everything else in the plane, especially if it is below deck where hundreds of suitcases and freight packages packed in foam make for pretty decent bomb-proofing. Also, I just mentioned how sturdy airplanes are on the bottom, so you have both a very strong wall and lots of energy absorbing material. Downstairs, therefore, you would need a much bigger bomb.

Less is needed if the bomb is placed next to the skin of the plane. There, the charge goes right against the outer wall of the plane. Additionally, the skin is much easier to breach in the passenger compartment than down below. This explains al-Qa'ida's use of window seats, especially ones above the wings, which hold the fuel tanks.

Just thinking through the placement issues allows you to segment an airplane into higher- and lower-risk zones.

Slide 10

Formula and Size

The next issue is what kind of explosive you need. We just talked about size, so you know that a larger bomb is needed in cargo or checked baggage. This has implications for how good security's detection capability needs to be. In other words, for items carried into the passenger compartment, where there is access to the skin of the aircraft, you need better detection that is able to find smaller amounts of explosives. Conversely, the scanning machines for cargo and baggage have a greater margin for error.

So size matters. If you bring on a bomb that is difficult to detect but ends up being too weak, you end up with a dud and are seized by the authorities, who can procure all kinds of intelligence from both you and the failed device.

Even if you get a bomb that is big enough, the exact formula is critical. In a lab, you can perfect the explosive, but it is riskier to ask an operative to carry on a ready-made bomb. While this probably is a more reliable device, it is easier to detect; for example, it might include a battery wired with a detonator sitting next to an explosive charge. Security officers can readily spot that combination. If, on the other hand, you break it down into undetectable pieces, the operative has to get the mix right—a large risk itself, especially since explosives can be extremely sensitive to even the most minute variation.

Slide 11

System Matters

Once you make the trade-offs about placement, size, and formula, there is the challenge of getting it all put together properly with power source, initiator, detonator, and explosive charge, not to mention the operative who has to get it all right in a high-pressure moment.

Pictured on the slide is the system that the 2006 liquid bombers planned to use on transatlantic flights from the UK to US and Canada.

In order to be successful, all the pieces have to be lined-up exactly right. Otherwise it doesn't work. The 2006 liquid plot would have killed thousands of people had not security authorities in the UK picked up the trail of the bombers as they prepared the plot.

Slide 12

A Flawed System

The Underwear Bomber is the inverse of the 2006 liquid bombers. He escaped detection long enough to get in the perfect position with his bomb, but the bomb system was flawed and did not work when the time came.

Abdulmutallab made mistakes in assembling and initiating the bomb and that contributed to its failure. Also, the formula of powder-based PETN, the same compound that was discovered in Richard Reid's shoe bomb) may not have had enough explosive punch to do the job, even next to the window.

The picture on the right is of a test chartered by the BBC and Discovery Channel using a mock-up of Abdulmutallab's bomb in perfect working order. What you see in the picture is a slight rippling of the skin, not a breach.

Even if everything went according to plan, why might have this bomb failed to carry out its intended purpose? The long carrying time in Abdulmutallab's underwear probably did not help the formula's effectiveness. Also, a chemical reaction underperformed in the detonator and the size and

shape of the bomb may not have had the necessary critical diameter to cause a large enough explosion.

In order to destroy a plane, the explosive needs to have enormous "pop," like C4's massive immediate punch. Other formulas, like Abdulmutallab's, don't have quite that burst: they're slower-acting and tend to burn rather than blow up.

In short, the Underwear Bomb was clever because it evaded detection, but ultimately the bomb did not, and I believe, would never, work.

So what do we learn from this? What does it show us about Inside-Out thinking?

Inside-Out thinking starts by asking: "what is needed to actually destroy the plane?" From there, you simply work backwards. The slides we just discussed show you some of the critical dependencies of getting a bomb that will, in fact, destroy its target.

How then, do we apply Inside-Out thinking to aviation security?

Slide 13

Reducing Exposure

First, I will run through a few examples of how Inside-Out risk management applies to aviation security.

Once you isolate the small subset of explosive size, formulas and system characteristics able to destroy a plane, you can reduce your exposure to them by several ways.

Start by using one effective Inside-Out approach: banning risky items. It turns out that liquid hydrogen peroxide-based explosives are very close to the center of the risk universe. They are easy to conceal and enormously powerful – if mixed right. The 3.4 ounces in a baggie rule came directly from asking: which formulas, in what size and put together how, could destroy an airplane? It was meant to stop these bombs from getting on board. Equally important, it was meant to push their bomb-makers out of the center of the risk universe, to the fringes of what might work.

Despite failures along the way, one could say that one of the things that saved the day on Christmas 2009 was the humble, unloved, one-quart, zip top, clear plastic bag known as the "baggie."

Slide 14

Expand, Deepen Defences

When thinking about risk Inside-Out, it becomes obvious that just protecting US flights from liquids is a lot of trauma for travelers that yields very little security benefit, since there is no cost to the al-Qa'ida plotter to originate a flight anywhere else in the world.

But because the European Union and, later, the International Civil Aviation Organization all adopted the same liquid restrictions, flights originating in Accra, Ghana; Lagos, Nigeria; Amsterdam,

Netherlands; and Detroit, Michigan all require al-Qa'ida bomb-makers to use something other than liquids in their bombs.

It is possible for the US to restrict liquids on flights coming to the US but it is a stronger system if it is enforced worldwide, which would result in a general shift away from using liquid bombs on flights.

Slide 15

Disrupt by Acting on Intelligence

Up until this point, we have only mentioned banning items as a way to disrupt al-Qa'ida's product development, but there are many other ways, as well. Here are two recent examples:

During 2007, there were disturbing indications that al-Qa'ida training camps were using remote control toys as camouflage for improvised explosive devices. These devices were determined to be potentially for use aboard commercial aircraft. When the intelligence "dots" became a threatening-looking pattern, TSA asked the National Counterterrorism Center (NCTC) to clear language that could be used in a public announcement. The Intelligence Community came together and acted in just a few days to make highly restricted intelligence useable to the public. The same technique was used again in 2010, this time in regards to thermoses and other insulated beverage containers, demonstrating that simple low-cost press releases can be effective counterterrorism tools. Clearly, we can disrupt terrorist product development by sending them a direct message that we know about their plotting and are taking specific measures against them. Though effective, this step can be extremely difficult to complete, as most classified intelligence comes with officials' reluctance to disclose it.

The key point here is that intelligence sources identified these objects as potentially threatening. The information was distributed in a timely manner and acted upon accordingly, neutralizing the potential threat.

Slide 16

Lots of Layers

Pretty much everyone agrees that layers are an integral part of any security programs. I would go a step further and propose that layers, for layers' sake, are themselves extremely effective counterterrorism measures.

Rather than have one line of defense that is thought to be impenetrable, you get a better security result from many different kinds of obstacles. In this case, any one layer might be beatable on its own, but together they are stronger than any conceivable layer. For example, if you have $1 million to spend, you get a better security result with a K-9 team ($150k), two Behavior Detection Officers to interview people ($500k) and a magnetometer with officers to conduct random pat-downs ($350k) than you do with one single $1 million scanner. The point is that there will inevitably be a weakness to the scanner—either it misses something or a terrorist evades it—whereas the other

system's overlapping measures would most likely catch somebody who slipped through one layer undetected. Additionally, layers are more effective at protecting against unknown threats. If you just put up layers based on what you think will happen, you make yourself vulnerable to threats you may not be aware of. Random measures are a good example of protecting against unknown threats. Had randomness been used with the explosives trace detection machines at the checkpoint used by Abdulmutallab on Flight 253, Abdulmutallab could not have known that he would escape the trace detection test. This could have stopped him right from the beginning.

SLIDE 17

"Inside-Out" Risk Management

The main point here is that thinking Inside-Out—starting with the worst possible outcome and working back to make that scenario impossible—is a useful tool in constructing a security program.

In the context of aviation, there are too many ways to harm an aircraft and too many flights (30,000/day, leaving close to 1,000 locations) to be able to (1) consider all of the potential hazards, (2) articulate them clearly, (3) circulate the information globally, (4) have them absorbed by tens of thousands of people all over the world, and (5) ensure that whatever recommendations you made are being carried out properly every time, everywhere. And when you eventually have to change strategy due to new intelligence or a new threat—well, then it becomes an entirely new problem.

If the goal were to LOOK like you are protecting air travel, perhaps this would be enough. But if you really want to stop attacks, you must use a different approach. Start with the worst-case scenario and work backwards to put up barriers to that outcome. Perhaps not everything is protected everywhere, at every moment, but taking the catastrophic 9/11-scale attack off the table is a worthwhile starting point.

So how does this differ from how aviation security works today?

SLIDE 18

"Outside-In" Problem Solving

The foundation of aviation security is regulatory. The TSA studies threats and vulnerabilities and takes into account consequence, latest intelligence and experience, as well as issues rules: rules for passengers, airlines, airports, freight companies, and other countries. These rules are based on traditional problem-solving, using a proven approach based on data analysis. This method starts by looking at the problem from an outside perspective and uses discipline and data to find the core of the problem.

In our Underwear Bomber case study, the process would determine that we have a terrorist enemy wanting to attack passenger aviation through blowing up planes or using them as weapons. We would then identify the precursors to such attacks – weapons and explosives – and keep them off planes. We use our regulatory power to make the rules and our enforcement capability, bolstered by technology and intelligence to accomplish the security mission.

This is an example of the Outside-In approach to security. We identify the core issue—in this case, no bombs on plans—and build and manage our process to prevent that from happening.

Slide 19

S.O.P. Kill Switch

The vulnerability of Standard Operating Procedure (SOP) security is that you have to write it down and depend on everybody getting it right in the execution. That can stifle imagination, judgment and brainpower.

Against an enemy who designs attacks around what you intend to defend, this can be a serious problem. It is dangerous to allow our focus on precise implementation of SOP to be a kill-switch for the brains of your frontline security personnel, at the TSA or anywhere else for that matter.

On the other hand, if you try to eliminate the weakness of SOP-based security, it's possible to veer too far in the other direction. If everybody is trained well, has access to current intelligence, is motivated to find the attack, and has the discretion in how to conduct the SOP, you run the risk of total chaos and disorganization. These are two conditions conducive to terrorist success.

So what do you do?

Slide 20

Keeping a Balance

In the end, it's all about balance. Successful security comes from making the following trade-offs:

- **"Outside-In" with "Inside-Out" security approaches.** This means that security and intelligence officials should try to identify potential threats by taking what they know and using it to guard against a **known** threat through regulation and standard process. They should also guard against the clever attacker who figures out a way around standard process by working backwards from the catastrophic event. This way we can interrupt elements critical to its execution regardless of whether we can figure out how they will get there.
- The consistency of **Standard Operating Procedures** with the flexibility of informed **Judgment**. Machines are capable of doing the same thing, the same way, perfectly. Humans are not, but the advantage that we have is that we can think and adjust in real-time whereas machines cannot. A machine's weakness can be found and exploited, like the X-Ray machine's inability to detect dangerous liquids. Security officers will make mistakes, but a terrorist planner cannot be sure that the right mistake will be made at the right place and time of his attack. Security officers who are well-trained and motivated can pick up on subtle clues that something is amiss– that is the unique human advantage over technology. If we believe that a security process can be 100% rule-based, we should use machines. Otherwise we should take advantage of the insight, judgment and experience that human officers provide.
- **Protection with public support.** By implementing security measures that are effective without being unnecessarily burdensome, as well as communicating as much as possible

with the public about restrictions and regulations, security and intelligence officials can foster an environment of trust and public confidence. If members of the public are engaged as active participants in the security process, that can provide more net security benefit than if the public tunes out and turns off in the face of “better, stronger” security procedures that are loathsome to the people being protected.

Terrorist attacks are considered a long-term threat for the TSA as well as any other federal, state and local department. Our open and dispersed society has targets at every turn and those responsible for our security have to make choices in deploying assets. Constructing a set security system and letting it run is a tempting approach because it can be monitored and measured. Such a system provides stability and consistency, but over time can become beatable. The best way we can sustain an effective security system is to keep moving, go on the offense and continually adapt to the ever-changing threat environment; in other words, to get—and stay—in balance.

Slide 21

Closing Credits

Music