Canadian Airport Security Review

Introduction

The aviation industry has received a considerable input of money since the crash of Air India Flight 182, the events of September 2001 and the Report of the Standing Senate Committee on National Security and Defence entitled, "The Myth of Security at Canada's Airports."[1] First, in the form of improvements in the realm of passenger baggage reconciliation and secondly by the fact that the industry has seen significant changes as regards the presence and supervision of security equipment and personnel.

Legislation passed immediately after the 9/11 tragedy transferred the security function of passenger and carry on baggage screening from the airline carriers to the new Canadian Air Transport Security Authority (CATSA) which was created as part of a comprehensive, $2.2 billion package of air security initiatives contained in the December 2001 budget. CATSA came into force on April 1, 2002, through Bill C-49.[2] CATSA is a Crown corporation based in the National Capital Region. It reports to Parliament through the Minister of Transport. Its mission is to protect the public by securing critical elements of the air transportation system as assigned by the government. In addition, 59 additional Transport Canada Security Inspectors across the five regions in the National Capital Region were hired, funding for aircraft security modifications of up to $30 million and a one time payment for increased police presence and security at airports (up to 20 million) were put into place.[3]

[1] Report of the Standing Senate Committee on National Security and Defence. (January 2003). The Myth of Security at Canada's Airports. Second Session Thirty Seventh Parliament.

[2] *Canadian Air Transport Security Act Statutes of Canada* 2002 c.9.

[3] Ibid.

This paper will focus on the breaches of airport security that led to the 1985 bombing of Air India Flight 182 and whether those breaches have been adequately addressed. I will also describe the events leading to the 1988 bombing of Pan Am Flight 103 over Lockerbie. There are significant cost effective measures that can be taken to prevent tragedies of this nature in the future. This paper will support the premise that the key to efficient aviation security is on the ground. Admittedly, every available tool in the tool box needs to be integrated into an overall security network, but the passenger baggage reconciliation is a solvable problem. The paper will review the procedures in place both before and after the Air India and Pan Am flights and some of the equipment available to screen passengers and baggage.

Air India Flight 182- 22/23 June 1985 Background

On June 16, 1985, a caller using the telephone number of the Ross Street Sikh Temple in Vancouver booked a single ticket for A. Singh to depart Vancouver via CP Flight 003 to Tokyo on June 22, 1985. The departing passenger was to connect with Air India Flight 301 in Tokyo. This ticket was never picked up because a change in plans was made to target two aircraft instead of just one. Three days later, a telephone caller spent a considerable time with a CP Air booking agent looking for suitable connecting flights to New Delhi for two people traveling in different directions from Vancouver. One passenger was to travel to New Delhi via Air India Flight 182 from Toronto and another via Air India Flight 301 in Tokyo. Three days later, and two days before the bombings, a man of East Indian descent wearing a saffron turban, arrived at the downtown ticket office of CP Air carrying cash. He paid for two tickets. Both were registered under the last name "Singh." One ticket was for passenger M. Singh flying from Vancouver to Toronto on June 22, 1985 via CP Air Flight 060 and connecting with Air India Flight 182 in Toronto. The other passenger, L. Singh, was to fly to Tokyo on the same day via CP Flight 003 and connecting with Air India Flight 301 from Narita to Bangkok. He paid $3005 cash for the two consecutively numbered tickets.[4] On June 22, 1985, a clean-shaven, well-dressed man lined up at counter 26 at Vancouver International Airport at around 8 a.m. and insisted the clerk direct-connect his bag with Air India Flight 182 in Toronto. The clerk originally said she could not do that because he was wait-listed. He was told that he was confirmed on Canadian Pacific Flight 060 to Toronto but was waitlisted for Air India Flight 181 Toronto to Montreal and then Air India Flight 182 from Montreal

[4] Bob Rae. (2005). Lessons to be Learned on Outstanding Questions with Respect to the Bombing of air India Flight 182, Ottawa: Air India Review Secretariat. .

to Delhi. The airline employee that checked the bag recalled that the man was particularly insistent that his bag be interlined all the way to Air India Flight 182. This was eventually done and there was no reconciliation check between records of bags and passengers before the flight took off; contrary to airline rules. The passenger argued and clerk relented. While his bag was boarded on the flight leaving from Vancouver, M. Singh did not board the aircraft but had a bomb in his checked baggage. At around 11 a.m. another Sikh lined up at the same counter to check in his bag for CP Flight 003 to Tokyo. Additionally, another airline agent checked in two pieces of luggage at the Vancouver International Airport containing a bomb .L.Singh's bag took off but the passenger did not board the flight. At exactly 6.13 (a.m.) GMT, a bag off-loaded from CP Flight 003 at Tokyo's Narita Airport exploded as it was being taken to waiting Air India Flight 301. The first suitcase exploded inside the baggage terminal at Tokyo's Narita Airport while being transferred to the Air India flight. Two baggage handlers are killed and four were wounded. Exactly 55 minutes later, the other bag, a dark-brown hard-sided Samsonite suitcase, exploded in the forward cargo hold of Air India Flight 182 as it approached the coast of Ireland. The flight disintegrated at altitude and the wreckage was scattered along a nine-mile swath of the ocean at 6,000 feet. The voice recorder showed there had been a loud bang aboard the aircraft. It also picked up the hissing sound of the fuselage opening up and a scream. The data recorders showed everything was normal on the aircraft until the explosion. The data recorder also showed a momentary control input by the pilot as he desperately tried to re-configure the aircraft. Some passengers actually survived the 747's fall from 31,000 feet only to drown in the frigid waters of the Atlantic. The attack killed 329 people, including 82 children. Among the victims are 280 Canadian citizens, mostly born in India or of Indian descent.

After the Air India crash, Canada was the first ICAO member to require passenger baggage reconciliation on international flights, which was later extended to domestic flights as well. Canada also initiated comprehensive background checks for airport workers and removal of baggage coin lockers from major airports. Cameras in and around security checkpoints were also banned. The current measures for checked baggage in 1985 were generally the same as existed prior to 2001 except that checked baggage on flights to the US must now be screened using a combination of explosive detections machines, physical means and conventional x-rays. By Jan 2006, all checked baggage from Canadian airports for any destination is subject to screening, however, the gap regarding cargo remains unchanged.[5]

Pan Am Flight 103- Lockerbie, Scotland- 21 December 1988- Background

The actual aircraft for Pan American Flight 103, a Boeing 747, N739PA, had originated in San Francisco. Many of the passengers arrived from Frankfurt, West Germany, on a Boeing 727, which had been positioned next to the Boeing 747. The passengers were transferred with their baggage to N739PA, which was to fly to New York. After a 6-hour turn around, the aircraft left Heathrow airport at 6:04 PM with 243 passengers and a crew of 16 on board. The aircraft exploded over Lockerbie, Scotland, and fell to the ground in pieces, killing 11 more innocent souls on the ground. Major portions of the wreckage fell over the town of Lockerbie and to the East. Smaller debris was strewn along two trails, the longest, which extended approximately 130 kilometers to the coast of England. The impact of the crashing plane was so strong that the British Geological Survey recorded a seismic event measuring 1.6 on the Richter scale.

Responsibility was originally thought to fall on the Popular Front for the Liberation of Palestine because of radio cassette bombs discovered in the hands of the PFLP-GC prior to the bombing. Many intelligence analysts were convinced that the Iranians were retaliating for the accidental shoot down of one of their commercial carriers. The latest evidence, however, indicated Muammar Khadaffi was really responsible. Law enforcement later discovered a significant clue. A link was established between an obscure case involving the arrest of Mohammed Marzouk and Mansour Omran Saber, both Libyan Intelligence agents, at Dakar, Senegal, airport in 1988 and the Lockerbie explosive device. It turns out they had in their possession 20 pounds of Semtex plastic, TNT explosives, weapons and some triggering devices. One of the triggering devices matched a microchip fragment from the Pan Am bomb. The circuit board fragment recovered from the crash was actually part of a sophisticated electronic timer. Senegalese authorities discovered the same type in the possession of the two Libyan terrorists who had been arrested in February 1988. Meister et Bollier, a Swiss electronics firm, specially manufactured the timers, designated as MST-13, and all 13 timers had been delivered to the Libyans. The perpetrators had made use of the Czech-made explosive

[5] Indian Kirpal Report, Report Of The Court Investigating Accident To Air India Boeing 747 Aircraft VT-ETO, "Kanishka" On 23rd June 1985.) and (Canadian Aviation Bureau Aviation Occurrence, Air India Boeing, 747-237B VT-EFO Report)

and very powerful Semtex. A double detonator device was used. The first trigger was activated by barometric pressure, which in turn activated a timing device. The actual bomb was encased in a Toshiba radio-cassette player. The terrorists were able to obtain and attach an appropriately marked Air Malta tag that enabled the luggage to circumvent baggage security measures and to be directly routed to the Pan Am feeder flight.

Forensic experts identified the bag that contained the bomb as a brown, hard-sided Samsonite suitcase. One of the defendants, Al-Megrahi, arrived in Valletta's Luqa airport, with the other defendant, Fhimah from Libya on the evening of 20 December 1988. Because Fhimah had been the former manager of the Maltese airport he had somehow retained full access to the airport. Scottish investigators traced the clothing that had been packed in the bag to a shop in Malta. Frankfurt airport records show that an unaccompanied bag was routed from the Air Malta Flight 180 to Frankfurt where it was eventually loaded onto the Pan Am Flight 103 feeder flight, as per perfectly legal procedures in effect at the time.

Other safety and security issues were also involved. Apparently a telephone threat, received from an anonymous caller on December 5 1988, at the American Embassy in Helsinki, Finland, warned of the impending disaster. The caller claimed a Finnish woman would carry a bomb aboard a Pan Am flight from Frankfurt to the US sometime during the next two weeks. US State Department sent out diplomatic traffic notifying its own personnel. Even though notice again was disseminated to all US consulates and embassies, since Finnish police determined it was a hoax, the information was not passed onto the FAA. The procedure of non-disclosure, which emerged from this incident and was persistently raised by the families of the victims, posed the question of exactly who should be advised in the event of threat information. The recommendation of the US President's Commission on Aviation Security and Terrorism in May 1990 was in favor of public notification of threats to civil aviation. However, security officials and the air carriers had reaffirmed an overall policy of nondisclosure.

The Lockerbie incident also raised the issue of passenger/baggage reconciliation. The President's Commission reported and concluded that passenger/baggage reconciliation is a bedrock component of any heightened security program. In 1988, Pan Am was x-raying all interlined bags rather than identifying and physically searching unaccompanied interline bags. Pan Am additionally claimed it had FAA approval to do this even though the FAA insisted it did not. Investigation disclosed the presence of an extra bag when the flight left Frankfurt, which had not been physically searched. It is unclear whether the bag had been x-rayed. This is important for Air India where the x ray machine broke down and investigators could not determine whether the bag was x rayed or not. Based on the recommendations of the Gore commission, US carriers were required to institute a strict bag matching policy to remove the baggage of any passenger who failed to actually board an aircraft. Canada did not institute these procedures until after the Air India crash. The process became fairly routine in the US, however not all overseas airlines and airports meet the requirements of such a program.

Many airlines now use a computer link between the luggage tag and the boarding pass; scanning the boarding pass when the passenger begins to actually board the aircraft and matching the individual to each piece of luggage. Again, not every airline in every city has implemented these procedures. If the airline determines that a passenger with checked baggage does not board the flight, the bags are located and removed from the flight, sometimes requiring significant delays. The process is known in the trade as "originating" passenger/baggage match. Meaning it is accomplished at the beginning of the first leg of the flight. Unfortunately, the process does not consider any bag that may already be in the cargo hold of the aircraft. If a person exits the aircraft during a stop over, the baggage may continue on without the passenger on board. Consequently, an originating passenger/baggage match system is really only a partial bag match if it does not reconcile the baggage and passengers already on board the aircraft after each and every stop. This, of course, could be administratively quite costly and time consuming. Checking interline bags would add additional costs to already expensive airline security measures. [6]

Comparisons and Dissimilarities: Procedures/Security Measures/ Equipment Air India

A check of CP Air's records and interviews with passengers indicates that the persons identifying themselves as M. and L. Singh did not board these respective flights. Air India Flight 181 from Frankfurt arrived at Toronto on 22 June 1985 at 1430 EDT (1830 GMT) and was parked at gate 107 of Terminal 2. All passengers and baggage were removed from the aircraft and processed through Canada Customs. Passengers continuing on the flight to Montreal were given transit cards, and on this flight, 68 cards were

[6] AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67.

handed out. These transit passengers are required to claim their luggage and proceed through Canadian Customs. Prior to entering the public area, there is a belt which is designated for interline or transit baggage. Transit passengers deposit their luggage on this belt which carries it to be reloaded on the aircraft. This baggage was not subjected to X-ray inspection as it was presumed to have been screened at the passengers' overseas departure point. When the transit passengers checked in to proceed to Montreal, their carry-on baggage was subjected to the normal security checks in place on this date. Passenger and baggage security checks were conducted by Burns International Security Services Ltd. and all passengers and baggage processing for both off-loading and on-loading was handled by Air Canada staff. It should be noted that some passengers from India book flights to Montreal with their intended destination being Toronto. The reason is that the fare to Montreal was cheaper and therefore some passengers get off the flight in Toronto, claim their luggage and leave without reporting a cancellation of the trip to Montreal. It has been established that 65 of the 68 transit passengers re boarded the flight to Montreal. Air India personnel were in charge for the overall operation at Toronto regarding the unloading and loading of both passengers and cargo. Although the actual work was performed by various companies under contract, Air India personnel oversaw the operation. The Air India station manager was away on vacation on 22 June 1985. The evidence does not clearly establish who had been assigned to replace the station manager and assume his duties. Furthermore, Air Canada had been storing an engine that had failed on a previous Air India flight from Toronto on 8 June 1985. Air Canada received a message from Air India stating that the failed engine was to be mounted as a 5th pod on Flight 181/182 on 22 June 1985. Due to problems with loading the 5th pod and component parts, the departure was delayed from 1835 EDT (2235 GMT) to 2015 EDT (0015 GMT, 23 June).[7]

CP Air Flight 060 arrived in Toronto at 1610 EDT (2010 GMT) and docked at gate 44, Terminal 1. A number of passengers on this flight were interlined to other flights including passenger M. Singh wait-listed on Air India Flight 181/182. It has been established that this passenger did not board Flight CP 060 but did check baggage onto the flight. This baggage was to be interlined to the Air India flight departing from Terminal 2. In this case, CP Air employees would have off-loaded all baggage from CP 060 and deposited the baggage at Racetrack 6 on the ring road of Terminal 1 to be

[7] AirDisaster.com, Special Report: Air India Flight 182: http://www.airdisaster.com/special/special-ai182.shtml.

transported to the Air Canada sorting room at Terminal 2. Consolidated Aviation Fuelling and Services (CAFAS) is a company which is contracted to pick up and deliver baggage from one terminal to the other. The CAFAS driver on duty at the time recalls picking up a bag from a CP Air flight originating in Vancouver and destined for Air India at Terminal 2. As this piece of luggage did not turn up as found luggage, it is deduced that normal practice was followed, and the luggage was interlined and loaded on AI 181/182. MEGA International Air Cargo is a firm that handled air cargo and containers for Air India. Since the flight was carrying a 5th engine and component parts, no commercial cargo could be loaded at Toronto. MEGA delivered the engine component parts to be loaded in the cargo compartment by Air Canada employees. Later, MEGA received two diplomatic bags and delivered these to the aircraft. The bags were loaded into the valuable goods container. These bags were not subjected to X-ray or any other security checks.

All checked-in baggage for AI 181/182 was to be screened by an X-ray machine which was located in Terminal 2 at the end of international belt number 4. This location would permit all baggage from the check-in counters and interline carts to be fed through the X-ray machine before being loaded. It has been established that this machine worked intermittently for a period of time and stopped working during the loading process at about 1700 EDT (2100 GMT). Rather than opening the bags and physically inspecting them, the Burns security personnel performing the X-ray screening were told by the Air India security officer to start using the hand-held PD sniffer. One Burns security officer checked the bags with the sniffer while another put stickers on the bags and forwarded them. The security officer forwarding the baggage recalls the sniffer making short beeping noises not long whistling ones. The security officer who used the sniffer claims it never went off, and the only time any sound was made was when it was turned on and off. At those times, it would emanate a short beep. Burns International Security had a contract with Air India for the security of the aircraft while it was docked. The security arrangements contracted from Burns were as follows:

- security at the bridge door leading to the aircraft;
- security inside the aircraft from the time the passengers disembarked upon flight arrival until flight departure;
- security guards assigned the physical inspection of all carry-on baggage in the departure room; and
- security guards in the international baggage make-up room conducting screening of baggage using an X-ray machine and a hand-held PD-4 sniffer.

The statements taken from Burns security personnel in Toronto indicated that a significant number of personnel, including those handling passenger screening, had never had the Transport Canada passenger inspection training program or, if they had, had not undergone refresher training within 12 months of the previous training. As a result of official requests made by Air India in early June 1985 for increased security for Air India flights, the RCMP provided additional security as follows:

- one member in a marked police motor vehicle patrolling the apron area;
- one member in a marked police motor vehicle parked under the right wing from time of arrival until push-back;
- one member on foot patrol at Air India check-in counter; and
- one member at the loading bridge during boarding.

In addition, all RCMP members working in that particular area of Terminal 2 were aware of the Air India flight and would check in with the assigned personnel during their patrols in the area of the aircraft and check in/ boarding lounges. Uniformed members were to patrol and monitor security within the airport premises Passenger check-in was handled for Air India by Air Canada under contract with Air India. The check-in included passengers originating in Toronto and interline passengers but did not include the transit passengers to Montreal. The check-in passengers were numbered using a security control sheet in accordance with instructions from Air India; however, the check-in and interline baggage was not numbered, and no attempt was made to correlate baggage with passengers. Hence, any unaccompanied interline baggage would not have been detected. The flight and cabin crew had been in Toronto for the week prior to this flight and were to take the aircraft to London where they would be replaced by another crew. The crew members themselves and their carryon baggage were not subjected to any security checks; however, their checked-in baggage was screened in the same manner as other baggage. [8]

Montreal

Air India Flight 181 from Toronto arrived at Mirabel International Airport at about 2100 EDT (0100 GMT, 23 June) and parked in supply area number 14 at 2106 EDT (0106 GMT). The 65 passengers destined for Montreal along

[8] Bob Rae. (2005). Lessons to be Learned on Outstanding Questions with Respect to the Bombing of Air India Flight 182, Ottawa: Air India Review Secretariat.

with three Air India personnel deplaned and were transported by bus to the terminal building. The remaining passengers remained on board as transit passengers and were not permitted to disembark at Montreal. Air Canada baggage handler's off-loaded four containers of cargo, three containers of baggage and a valuables container.

Two diplomatic pouches from the Indian High Commission in Ottawa were delivered to the aircraft by MEGA International Cargo. One pouch weighing one kilogram was hand-delivered to the flight purser for storage in a valuables locker within the cabin and the other pouch was loaded into the valuables container. At about 1730 EDT (2130 GMT), Air Canada, which is Air India's contracted agent, opened its check-in counter to passengers who would be flying on Air India Flight 182. Burns security personnel were also assigned at this time to screen the checked baggage. Passenger tickets were checked, issued a number, and copies of the tickets were removed and retained by Air Canada. Boarding passes were then issued and affixed to the numbered tickets. Also attached to the ticket booklets were numbered tickets which corresponded to each piece of checked baggage. The numbered checked baggage was sent to the baggage area by Air Canada personnel to be security-checked by Burns security personnel. The passengers for AI 182 after checking in were free to enter the departure area. At the entrance to the departure area, Burns security staff used X-ray units and metal detectors to screen passengers and carry-on baggage. At about 2100 EDT (0100 GMT), the passengers proceeded to gate 80 where they gave their boarding passes and numbered tickets to an Air Canada agent. The agent kept the numbered flight tickets and checked the numbers against the passenger list. Also, at gate 80, a secondary security check was done on passengers by a Burns security officer using a metal detector. Hand-carried baggage was subjected to further physical and visual checks. A total of 105 passengers boarded the flight at Mirabel Airport; there were no interline passengers. Between 1900 (2300 GMT) and 1930 EDT (2330 GMT), Burns security personnel identified a suspect suitcase using the X-ray machine. The suitcase was placed on the floor next to the machine. The Burns security supervisor told Air India personnel that a suspect suitcase had been located and was advised within 15 to 20 minutes to wait for the Air India security officer who would be arriving on the flight from Toronto. Subsequently, a second suspect suitcase was identified and a little later a third. The three suitcases were placed next to the X-ray machine. Between 1930 (2330 GMT) and 1945 (2345 GMT), all the Burns security personnel at the X-ray machine were assigned to other duties and the three suspect suitcases remained in the baggage area without supervision. At about 2140 (0140 GMT), the Air India security officer went to the baggage room and inspected the three suitcases with the X-ray machine and a sniffer that was in the possession of the security officer. The Air India security officer decided to keep the three suitcases and, if further examination proved negative, send them on a later flight.

At approximately 2155 (0155 GMT), the Air Canada Operations Centre supervisor contacted the airport RCMP detachment regarding the suspect suitcases. At about 2205 (0205 GMT), an RCMP member located the suitcases in the baggage room and requested that an Air India representative be sent to the baggage room. About five minutes later, the Air India security officer contacted the baggage room by telephone and advised that he could not come to the room immediately. The Air India security officer arrived in the baggage room at about 2235 (0235 GMT) and, when asked to determine the owners of the suitcases, informed the RCMP member that the flight had already departed [2218 (0218 GMT)]. The three suspect suitcases were later examined with negative results. The remainder of the checked baggage which cleared the security check was identified by a green sticker. The baggage was then forwarded to Air Canada personnel who loaded the baggage in containers to be placed on board the aircraft. A later check with Canada Customs and Air Canada at Mirabel revealed no unclaimed baggage associated with AI 181/182. A similar check at Dorval Airport was conducted with negative results. No record was kept as to the location and number of individual pieces of checked-in luggage. Records were kept as to the location of the containers according to destination, where loaded and the number of pieces of luggage in each container. The Mirabel Detachment of the RCMP provided the following security at the airport on 22 June 1985:

- one member in a police vehicle for airside security;
- one member on patrol in the arrival and departure areas;
- one member on general foot patrol throughout the terminal; and
- one member as a telecommunications operator in the detachment office.

In addition, due to the increased threat to Air India flights, the RCMP provided the following supplementary coverage to Air India Flight181/182 on 22 June 1985:

- one member in a police vehicle escorted the aircraft to and from the runway and the terminal building and remained with the aircraft while it was stationary;
- one member in a police vehicle remained at the entrance to the ramp;
- two members patrolled the area of the ticket counter and access corridors, and one of these members also served in a liaison capacity with the airline representatives.[9]

Pan Am Flight 103

There was an explosion in the forward cargo compartment which caused an explosive decompression that led to the in flight breakup of Pan Am Flight 103. The combined effect of the direct and indirect explosive forces was to destroy the structural integrity of the forward fuselage.' This disaster occurred as a result of a bomb, an improvised explosive device," being placed within a Toshiba radio situated in a brown Samsonite suitcase. The location of the suitcase established that it was an interline bag; namely it had come from another carrier and had been placed on the Pan Am flight at some point in its journey. From its location, it was established it could only have been loaded on the airplane at Frankfurt, Germany. Furthermore, the baggage tags led to a precise paper rail which established that the bag in question was an interline transfer bag from Air Malta Flight 180. The unaccompanied bag was placed on Pan Am 103 A, a feeder flight, and was transferred to Flight 103 at Heathrow Airport, outside London. The bags transferred from Pan Am 103A were taken directly from that aircraft to Pan Am 103, and that they were not counted or weighed. Additionally, they were not reconciled with the passenger manifest, and they were not x-rayed at Heathrow. Thus the bag, which was loaded at Frankfurt, traveled to London and was loaded on Flight 103 without being identified as an unaccompanied bag. Additionally, two Libyans, including the Libyan Arab Airlines station manager at Malta, who had unlimited access to the baggage area for all Air Malta flights were investigated. Libyan Airlines used the same baggage tickets as Air Malta, and on December 21, 1988, the Libyan Airlines flight to Tripoli was processed at the same time and at the same counter as Air Malta Flight 180. Moreover, the security procedures at Malta were symbolic at best.

[9] AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67, RA-5C,

FAA Security Requirements (overseas) pertinent to Pan Am crash

Positive passenger baggage reconciliation was long recognized as an important element in the system designed to prevent the carriage of unaccompanied bags. Unaccompanied bags were a well-established method used by terrorists to get bombs on board airline flights. The Federal Aviation Administration (FAA) required a positive match of bags to boarding passengers in airports which were classified as extraordinary security risks airports. Frankfurt and London had been categorized by the FAA as falling into that category. Under FAA rules, once an unaccompanied bag was identified at one of the high risk locations, it could only be carried on board an aircraft if physically searched. Pan Am had abandoned this positive matching process without written approval in February 1987, at Heathrow and in July 1988, at Frankfurt. Without permission from the FAA, Pan Am had substituted what they described as an administrative match and positive passenger control. The new administrative match and positive passenger control system was inadequate because it did not deal with interline bags. Pan Am was aware of their duty to meet the FAA Regulations. The rule was contained in their manuals as required by law. The decision to ignore the rule was taken at the highest corporate level. [10]

Warnings/Issue

In April 1988, the FAA warned all international airlines of intelligence reports of threats by Iran against United States targets. On November 18, 1988, Pan Am was advised by an FAA Security Bulletin that a Middle Eastern terrorist group had been found in Germany with a bomb concealed within a Toshiba radio. The alert called upon Pan Am and other airlines to activate extra vigilance and a rigorous adherence to their regulations for baggage reconciliation. Pan Am and others were warned of the difficulty of relying on x-rays which would not detect such bombs. Despite this explicit warning, Pan Am did not positively match interline bags, even worse, the ALERT security staff in Frankfurt was not made aware of this warning. Not even the personnel using the x-ray equipment were told of this warning. They did not know, and were unaware of what to look for. On December 7, 1988, only two weeks before the Lockerbie disaster, Pan Am was issued a Security Bulletin advising that the United States Embassy in Helsinki, Finland, received a warning that a Pan Am flight from Frankfurt to the United States would be the target of a bomb. The notice became known as the Helsinki

[10] AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67, RA-5C,

Warning. It referred to and reiterated the FAAs earlier warning of a Toshiba radio bomb and again emphasized the difficulty of detection by x-ray. Once again the security personnel at Frankfurt, including ALERTs chief of training, were not informed of the bulletin. Pan Am not only failed to increase security staff, they failed to alert the on duty security staff to the warnings. When he eventually received the Helsinki Warning, the manager at Frankfurt attempted to back date it and to suggest that he had disseminated it. He had not.

Frankfurt

Pan Am had their own security and baggage handling staff. There was a computer controlled automated baggage handling system. Each item of baggage was placed in an individually numbered tray as it was taken into the system. The trays were placed on conveyor belts and instructions were fed into the computer to identify the flight to which the baggage was to be sent, the position from which the aircraft was to leave and the time of the flight. The trays were dispatched to a waiting area where they circulated until an instruction was fed in to summon the baggage for a particular flight, whereupon the items would be automatically extracted from the waiting area and sent to the departure point. Local origin baggage was received at check-in desks, and passed into the system. Transit baggage was taken to one of two areas, known as V3 and HM, where it was fed into the system at points known as coding stations. There were seven coding stations in V3. The general practice was that baggage from an incoming flight was brought either to HM or to V3 in wagons or containers and would be directed by an employee called the interline writer to one or more of the coding stations. The proper practice was that each coding station should not deal with baggage from more than one incoming flight at a time. Normally there were two employees at each coding station. One would lift the items of baggage from the wagon or container and place each item in a tray. The other would enter into the computer, in a coded form, the flight number and destination for the outgoing flight, taking the information from the tag attached to the item. Records were kept identifying the staff working at particular stations, the arrival times of aircraft, the arrival times of consignments of baggage at HM or V3, and the station or stations to which the baggage from a particular flight was sent. The computer itself retained a record of the items sent through the system so that it was possible, for a limited period, to identify all the items of baggage sent through the system to a particular flight. The computer controlling the baggage handling system contained its own clock, which had a tendency to diverge from real time. It was reset at the start of each day, but by 1600 or 1700 hours the discrepancy might be as much as two or three minutes. Times entered in records not generated by the computer were obtained by the staff from the airport clock or from their own watches.

Pan Am had x-ray equipment at Frankfurt, which was used to x-ray interline baggage. The practice of Pan Am at Frankfurt was to carry out reconciliation between local origin passengers and baggage and online passengers and baggage, to ensure that every such passenger who had baggage on the flight was accounted for, but there was no attempt to reconcile interline passengers and their baggage. Flight KM180 reached its parking position at 1248 hours on 21 December 1988. It was unloaded by employees of the airport authority. According to the record, the unloading took place between 1248 and 1300 hours. Andreas Schreiner, who was in charge of monitoring the arrival of baggage at V3 on that day, recorded on the interline writer's sheet that one wagon of interline baggage from flight KM180 arrived at V3 at 1301 hours. A coder, Yasar Koca, was working at station 206 in V3. He completed a worksheet which showed that one wagon of baggage from flight KM180 was coded at station 206 between 1304 hours and a later time which the trial court held to be 1310. No passenger on flight KM180 had an onward booking from Frankfurt to London or the United States. All the passengers on the flight retrieved their checked-in baggage at their destinations. The Malta documentation for flight KM180 did not record that any unaccompanied baggage was carried. There was, however, evidence that there was an item of baggage which was neither accompanied nor otherwise accounted for. A computer printout relating to baggage sent for loading onto flight PA103A bore to record that an item which had been placed in tray number B8849 was coded at station 206 at 1307 hours and was transferred and delivered to the appropriate gate to be loaded on board flight PA103A. There was a plain inference that an unidentified and unaccompanied bag traveled on flight KM180 from Luqa airport to Frankfurt and there was loaded on flight PA103A. Flight PA103A departed for London at 1653 hours. The Air India crash procedures in effect at the time of the incident represent, in conjunction with Lockerbie, failures in the interline security protocols.

Legal Issues

International Standards and Recommended Practices

International security standards and recommendations to safeguard international civil aviation against acts of unlawful interference are listed in ICAO Annex 17 to the Convention on International Civil Aviation. Suggested security measures and procedures are amplified in the ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference. [11]Annex 17 requires contracting States of which Canada is one to "take the necessary measures to prevent weapons or any other dangerous devices, the carriage or bearing of which is not authorized, from being introduced by any means whatsoever, on board an aircraft engaged in the carriage of passengers." In addition to other recommendations, Annex 17 recommends that contracting States should establish the necessary procedures to prevent the unauthorized introduction of explosives or incendiary devices in baggage, cargo, mail and stores to be carried on board aircraft. These proposals arose from a decision taken by the Council in its 115th Session on 10 July 1985. The Council instructed its Committee on Unlawful Interference, as a matter of urgency, to review the entirety of Annex 17 and to report on those provisions which might be immediately introduced, upgraded to Standards, strengthened or improved. Among the proposed amendments is the following upgrading in the Standards: - Each contracting State ensures the implementation of measures at airports to protect cargo, baggage, mail stores and operator's supplies being moved within an airport to safeguard such aircraft against an act of unlawful interference.

Canadian Law

In terms of Canadian statutory requirements, the Civil Aviation Security Measures Regulations and the Foreign Aircraft Security Measures Regulations made pursuant to the Aeronautics Act require specified owners or operators of aircraft registered in Canada or specified owners or operators who land foreign aircraft in Canada to establish, maintain, and carry out security measures at airports consisting of:

[11] Convention on International Civil Aviation. Suggested security measures and procedures are amplified in the ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Annex 17.

- systems of surveillance of persons, personal belongings, baggage, goods and cargo by persons or by mechanical or electronic devices;

- systems of searching persons, personal belongings, baggage, goods and cargo by persons or by mechanical or electronic devices;

- a system that provides, at airports where facilities are available, for locked, closed or restricted areas that are inaccessible to any person other than a person who has been searched and the personnel of the owner or operator;

- a system that provides, at airports where facilities are available, for check-points at which persons intending to board the aircraft of an owner or operator can be searched;

- a system that provides, at airports where facilities are available, for locked, closed or restricted areas in which cargo, goods and baggage that have been checked for loading on aircraft are inaccessible to persons other than those persons authorized by the owner or operator to have access to those areas;

- a system of identification that prevents baggage, goods and cargo from being placed on board the aircraft if it is not authorized to be placed on board by the owner or operator; and

- a system of identification of surveillance and search personnel and the personnel of the owner or operator.

Specified carriers including Air Canada, CP Air, and Air India were required to provide a description of their security measures to the Canadian Minister of Transport. An Order-in-Council on 29 September 1960 established that the RCMP was responsible for the direction and administration of police functions at major airports operated by Transport Canada. The duties of the Police and Security Detail at these designated airports include the following:

- carry out policing and security duties to guard against unauthorized entry, sabotage, theft, fire or damage;

- enforce federal legislation;

- respond to violations of the Criminal Code of Canada, Federal,

- Provincial, and Territorial statutes, and perform a holding action pending arrival of the police department having primary criminal jurisdiction;

- man guard posts; and provide a police response in those areas of airports where pre-board screening takes place. Section 5.1(9) of the Aeronautics Act stated that "The Minister may designate as security officers for the purposes of this section any persons or classes of persons who, in his opinion, are qualified to be so designated." Pursuant to this section Transport Canada has established criteria for persons or classes of persons that are designated as security officers in a Schedule registered on 11 April 1984. The criteria also specify that a security guard company and its employees will meet Transport Canada requirements provided that the company:

- is under contract with a carrier to conduct passenger screening under the Aeronautics Act and Regulations;

- is licensed in the province or territory;

- complies with the security guard criteria as follows in that the guard must:

- be 18 years or older,

- be in good general health without physical defects or abnormalities which would interfere with the performance of duties,

- be licensed as a security guard and in possession of the license while on duty, and

- meet the training standards of Transport Canada consisting of successfully completing the Transport Canada passenger inspection training program, attaining an average mark of 70 per cent, and undergoing refresher training within 12 months from previous training;

- uses a comprehensive training program which has been approved by Transport Canada and is capable of being monitored and evaluated;

- keeps records showing the date each employee received initial training and/or refresher training and the mark attained; and

- provides supervision to ensure that their employees maintain competency and act responsibly in the conduct of searching passengers and carry-on baggage being carried aboard aircraft. [12]

Canadian Security Procedures

In accordance with the Canadian Aeronautics Act and pursuant regulations, air carriers are assigned the responsibility for security. Transport Canada provides the following security services for the air carriers using major Canadian airports, including the international airports in Vancouver, Toronto and Montreal:

- security and policing staff including RCMP airport detachments;

- specific airport security plans and procedures;

- secure facilities (e.g., secure areas, pass identification systems, etc.); and

- security equipment and facilities (e.g., X-ray detection units, walkthrough metal detectors, hand-held metal detectors, explosive detection dogs).

[12] *Canadian Air Transport Security Act Statutes of Canada*

- As of 22 June 1985, the following general security measures were in place at Canadian airports:

- metal detection screening of passengers; and

- X-raying of carry-on baggage.

Checked baggage was not normally subject to any security screening. A few air carriers such as Air India had extra security measures in place because of an assessed higher threat level

On 23 June 1985, Transport Canada required additional security measures to be implemented by all Canadian and foreign air carriers for all international flights from Canada except those to the continental United States. These measures required:

- the physical inspection or X-ray inspection of all checked baggage;

- the full screening of all passengers and carry-on baggage; and

- a 24-hour hold on cargo except perishables received from a known shipper unless a physical search or X-ray inspection is completed. Further, on 29 June 1985, Transport Canada directed that all baggage or cargo being interlined within Canada to an Air India flight was to be physically inspected or X-rayed at the point of first departure and that matching of passengers to tickets was to be verified prior to departure.[13]

Air India Security Program in Canada

In accordance with the Foreign Aircraft Security Measures Regulations, Air India had provided the Minister of Transport with a copy of its security program. It included measures to:

- establish sterile areas;

- physically inspect all carry-on baggage by means of hand-held devices or X-ray equipment;

[13] Bob Rae. (2005). Lessons to be Learned on Outstanding Questions with Respect to the Bombing of air India Flight 182, Ottawa: Air India Review Secretariat.

- control boarding passes;
- maintain aircraft security;
- ensure baggage and cargo security; and
- off-load baggage of passengers who fail to board flights.

Under these procedures established by Air India, passengers, carry-on baggage, and checked baggage destined for AI 181/182 on 22 June 1985 were subjected to extra security checks. A security officer from the Air India New York office arrived in Toronto on 22 June 1985 to oversee the security operation at Toronto and Montreal. On 17 May 1985, the High Commission of India presented a diplomatic note to the Department of External Affairs regarding the threat to Indian diplomatic missions or Air India aircraft by extremist elements. Subsequently, in early June, Air India forwarded a request for "full and strict security coverage and any other appropriate security measures" to Transport Canada offices in Ottawa, Montreal and Toronto, and RCMP offices in Montreal and Toronto.[14]

PD-4 Sniffer/Issue

On 18 January 1985, prior to the inaugural Air India flight out of Toronto on 19 January, a meeting on security for Air India flights (Toronto) was held with representatives from Transport Canada, RCMP and Air India. At this meeting, a PD-4 sniffer belonging to Air India was produced. It was explained that it would be used to screen checked baggage as the X-ray machine had not yet arrived. At that time, an RCMP member tested its effectiveness. The test revealed that it could not detect a small container of gunpowder until the head of the sniffer was moved to less than an inch from the gunpowder. Also, the next day the sniffer was tried on a piece of C4 plastic explosives and it did not function even when it came directly in contact with the explosive substance. It is not known if this was the same sniffer used on 22 June 1985.

US Law/FAA Regulations

Prior to 9/11 air carriers had the responsibility to prevent and deter carriage of weapons and explosives aboard their aircraft by potential hijackers. Where applicable, air carriers issued and carried out written

[14] Ibid

security programs, which accomplished 100 percent screening of all passengers and searched all carry-on items.[15] Post 9/11, this basic concept has been expanded to require all baggage be screened by explosive detection equipment before 31 December 2002, not by airlines but by the government. Conversely, airports serving applicable air carriers are responsible for preventing and deterring unauthorized access to the air operations area, and for providing law enforcement support at passenger screening stations. Basically, Federal Aviation Regulation, Parts 107 and 108 required airport operators and airlines to issue a security program incorporating the above procedures. Overall, the FARs set the general guidelines for all security assets and procedures at US airports and for US and foreign airlines servicing US airports.

Police Support

On 1 April 1981, the FARs were amended as Sec 107.15 to state: Each airport operator shall provide law enforcement officers in the numbers and in a manner adequate to support

1. Its security program; and

2. Each passenger screening system required by Part 108 or Sec 129.25 of this chapter. 49 CFR Chapter XII Part 1544.217, (Nov 2001) requires each airport operator to arrange for law enforcement personnel meeting the qualifications and standards specified in Section 1544.21 and provide its employees current information regarding procedures for obtaining law enforcement assistance at that airport. Basically, it means that law enforcement personal should be made available within a reasonable period of time.

Passenger and Baggage Screeners

The sterile concourse establishes an area to which access is controlled by the inspection of persons and property in accordance with an approved security program. Passengers have come to accept them as the normal course of business in an airport. At most airports, security operations are located at a central screening point at the central access point to a concourse, which serves several gates. This negates the need for

[15] FAR Part 121.538 and Part 108.7. *Note: Current regulations are contained in 49 CFR Chapter XII, Parts 1540 et al.*

airport authorities to bear the costs of maintaining security personnel at each gate or to station a law enforcement officer at each gate. This simple change of location from the gate to the choke-point before the concourse entrance eventually made the practicality of x-ray machines to search baggage practical. The cost of an x-ray machine at each gate was a severely costly proposition. X-ray screening only became practical with the improvement of technology and the increase in number of businesses manufacturing them.

Now all sorts of x-ray machines and walk-through or hand held metal detectors have resulted in a tremendous economy of equipment and personnel. Fewer pieces of equipment and, more importantly the need to employ fewer people to operate them, has arguably furnished the greatest savings. Cost related problems have however resurfaced with the high cost of explosion detection systems and the requirement to screen all checked baggage by the end of 2002. It has become clear that airport baggage areas, not the ticket counters, provide a better venue for the location of the newly mandated explosive detection equipment. This will require extensive renovations to some airports. However, placing the explosive detection equipment in the baggage area makes the screening invisible to the passenger and eliminates unnecessary congestion at the check-in and passenger screening points. This sequence becomes part of the normal process of transferring the baggage from the ticket counter to the airplane.

In the past, a vast majority of the people operating baggage and passenger screening systems in airport terminals were contract security guards. The airlines hired airport security firms to conduct essential searches and passengers depended on their expertise to maintain the safety of airports and aircraft around the globe. They were poorly trained and poorly paid, often only receiving minimal training. Their training often consisted of instruction on the operating systems and procedures by someone simply employed longer than the new employee. The instructor or supervisory employee probably did not have very extensive experience, considering most contract firms experienced a 100% turn over rate per year or more. Demographically, they were young, women, retired and/or are representative of a minority segment of the population. Frequently, English or French was their second language. It was ironic that the public relied so heavily on the dedication of these people for their safety and security but failed to reciprocate with appropriate compensation in order to attract more qualified personnel.

In Canada, CATSA immediately began the process of hiring and training personnel to man the security stations at airports. They were faced with the same problems which previously challenged private security firms. In the US, the TSA, is facing those same problems. It now operates most of the US passenger screening process and is tasked with analyzing threats that pertain to the entire transportation infrastructure, aviation related and otherwise. In the US, the GAO had published a report in 2000 clearly portraying the inadequate security previously provided. The report indicated that turn over among personnel was a huge problem. Specifically, the report stated that, "from May 1998 through April 1999, screener turnover averaged 126 percent at 19 of the nation's largest airports."[16]

In another report dated December 2000, The Department of Transportation's Inspector General stated that too many airport employees with unknown or questionable backgrounds are given access to secure areas. "Randomly pulling workers' files at six airports, investigators determined that 16 percent had undergone incomplete background checks and 8 percent had no checks at all."[17] Years previously, there had been some additional alarming studies on the need for improving security at US airports. In 1987, an FAA evaluation at major airports discovered that screeners missed approximately 20% of the potentially dangerous items which passed in front of them. Another study revealed the chilling statistics that screeners in European airports detected twice as many test objects as US screeners. A FAA report concluded that, "people who had longer training, somewhat better pay and benefits, and better on-going testing by screening companies, had much better performance in detecting objects than comparable screeners in the US."[18] In addition, the caretakers of security at airports, unfortunately, were not above being bribed, engaging in criminal activities or just being non-committed to the job. These circumstances often resulted in significant laxness in security. The situation has not really changed all that much in spite of 11 September. Security at London's Heathrow Airport was overhauled in March 2002 after two multi-million dollar heists in a two-month period. The British government announced more stringent background checks on employees, tighter restrictions on access to sensitive areas and now

[16] Sweet. Kathleen. (2003). Aviation and Airport Security: Threats and Safety Concerns, Upper Saddle River, NJ: Prentice Hall Publishers, pg 209.

[17] Morris, Jim, "Since Pan Am 103, a Façade of Security", *U.S. News*, 19 February 2001, Internet: http://www.usnews.com/usnews/issue/010219/safety.htm, Pg. 1-3.

[18] Rochelle, Carl, "FAA Calls for Security Improvements at US Airports", Internet: http://www.cnn.ru/2000/_travelnews/01/07/bomb and baggage, 7 Jan 2000.

requires security companies to be on an approved list. The job as an airport security guard was not one that children aspired to become while growing up. As mentioned, more often than not, the job paid poorly, provided little chance for advancement or promotion and most likely provided little training for those that were even somewhat dedicated to the job. On top of that, the screeners were frequently subjected to verbal abuse by passengers, airline employees, allegedly by government personnel and by their own co-workers. In fact, a report cited this abuse as the most regularly cited cause of leaving the job, as opposed to low pay and virtually no benefits. It is fair to assume that Canada suffers from these same problems.

Poor operator performance continues to be another principal weakness of passenger screening systems. Airport security screeners, who are preoccupied with inter-personal problems on the job and poorly trained, are still required to identify sometimes faint indications of infrequently appearing target items. Missing such indicators can have catastrophic results if a bomb or other explosive device survives the screening process. This problem will remain and will prove challenging to authorities. The relationship between pay and performance is not necessarily a determinative one. Experts would argue that increased pay is not likely, in and of itself, to solve the problem. The government must place a renewed emphasis on attaining job effectiveness goals. This process will likely involve the application of two types of factors. Those factors will consist of those that attract and keep people on the job (maintenance factors) and those that lead to acceptable or enhanced performance on the job (performance factors). [19]

Another challenge relates to the self- perception of people hired in this field. Higher levels of pay will possibly make up for poor working conditions, but do not enhance the perceived low status of the job. Improved training techniques will greatly improve this aspect. Even the weekly access to “intelligence” briefings on the assessed threat by qualified personnel will improve job satisfaction. People who believe they are actually important and contributing to combating a real threat will often live up to the challenge. Those employees referred to as “rent-a-cops” will not.

[19] Guzzo, R.A., 1988, *Productivity in Organizations*, Jassey-Bass: San Francisco, CA.

The use of trace detection technologies and explosive detection systems will also require specialized training. Trace detection equipment requires the use of specific protocols to be effective. Additionally, passenger screening settings may involve person to person contact or direct contact between the equipment and the passenger. Additionally, operators may feel intimidated by passengers. Training regarding the management of anger will also prove quite useful. To facilitate training of screeners, the deployment of a computerized training system called Screener Proficiency Evaluation and Reporting System or SPEARS has proved effective. One unique aspect of the system is a concept known as Threat Image Projection (TIP), which consists of specific software to project fictitious images of bags with threat devices on x-ray screens to keep screeners alert and measure performance in real-time conditions. Governments will likely continue the use of these systems.

It is also important to recognize the distinction between state appointed law enforcement officers and "private" security officers. There are four basic differences. The significant distinctions include financial sourcing, profit orientation, goals toward crime prevention vs. protection of assets and the possession of statutory authority. Private security is employed by profit-oriented businesses. The police are statutorily appointed or sworn-in the service of the public and are paid by governments. Additionally, police officers are often focused on the investigation of crime that has already taken place or is taking place. Private security officers are supposed to focus on crime prevention and the protection of assets belonging to the business. The functions are similar and do overlap but the motivational differences are worthy of note. Furthermore, training for law enforcement in the very complicated airport arena is recommended.

Interim Conclusions: Passenger Baggage Reconciliation

Subsequent to the Air India 182 crash, several recommendations proceeded from the resulting Indian-Canadian reports. One of the most important called for the **complete** reconciliation of all checked baggage to all on-board passengers before flight This recommendation, however, was never fully implemented for international flights across the industry until the similar loss by explosion of Pan Am Flight 103 over Lockerbie, Scotland, in 1988. Arguably, the issue of cost impinged efforts to correct these problems in 1985. In addition, the reconciliation of passengers to bags for domestic flights was not implemented, in the North American context, until after the events of 9/11. This latter delay was a by-product of the cost and "operational penalties" associated with the reconciliation of domestic baggage, which is to say that reconciliation takes time [20]

On one end of the spectrum is El Al who, by the time of the Air India 182 incident, had implemented a layered, defence-in-depth security system that put integrated measures in place throughout its operational environment. On the other is the North American civil aviation industry, which, subsequent to the same event, seemed to implement security measures in a reactive, after-the-fact fashion. The reasons for these variations in approach can be related to the balance struck between the perceived need for change and the cost or effort involved in making change happen.

In Canada, the formation of the Canadian Air Transport Security Authority (CATSA) in 2002 became the centerpiece of a reconfigured aviation security system. This development, however, did not seek to address the command-and-control issues that preceded it. The overall system remains fractured. A chief executive officer (CEO) heads the current CATSA system. A Board of Directors oversees the CEO. The board currently comprises 11 individuals, including its chairperson. A dedicated general counsel and three vice-presidents assist the CEO in his responsibilities: there is currently one VP for corporate affairs, one for public affairs, and one for operations. The command-and-control network below this hierarchy is distributed amongst 89 designated Canadian airports. Ten individuals serve as "facilitators" to the nine major or Class 1 aerodromes, while 14 regional managers attend to the remaining Class 2 and 3 facilities (CATSA, 2002). As the Senate Committee for National Security and Defence observed: "A maze-like matrix of departments, agencies and corporations hold responsibilities for security at Canadian airports, and there is a fuzzy Alphonse-and-Gaston relationship between the public and private sector as to who will be responsible if security all goes haywire." [21]With overlapping and ambiguous responsibilities, the command-and-control arrangements within the Canadian civil aviation security sector need to be revisited.

Security Requirements

Given the assumed terrorist threat to Canada, Canadian citizens, institutions, and economic capabilities, the existing security systems in

[20] Wallis, Rodney. (2000). Lockerbie the Story and the Lessons. Praeger Publishers.

[21] Report of the Standing Senate Committee on National Security and Defence. (January 2003). The Myth of Security at Canada's Airports. Second Session Thirty Seventh Parliament.

the Canadian civil aviation industry must present a seamless, coordinated, and effective defence. An effective security organization needs to be able to counter this threat at any point in the operational matrix. This is an onerous task because of the large number of agencies involved and the boundaries that separate them—boundaries that are particularly sensitive to exploitation. An effective security system needs to be able to make plans that address the relevant threats. A relevant threat is one that has both the capabilities and intentions of inflicting damage within the aviation environment; identify the threat before it is able to inflict damage; alert the operational system and organize security forces to react to this threat; direct security forces to engage and defeat the threat; and continuously monitor, test and improve security system capabilities to defeat an adaptable and evolving threat. The making of plans to address the relevant threats presupposes an ability to gather related information and make informed recommendations on how the threats can be defeated.

Challenges

As stated, the Canadian Air Transport Security Authority (CATSA) administers Canadian civil aviation security responsibilities. A review of the enabling legislation [22] reveals that this agency is having some difficulty in bringing into effect the requirements of a new security system. This legislation indicates that a not-for-profit Crown Corporation is to be primarily concerned with traditional airport security services. These functions revolve around the provision of passenger and baggage screening services with little emphasis on airborne security measures. Indeed, the original CATSA mandate was modified to accommodate the introduction of armed air marshal services as directed by American authorities and as requested by the Air Canada Pilot's Association [23] The Crown Corporation is remote from publicly-controlled intelligence, enforcement, and regulatory agencies, which will make planning unnecessarily difficult. Likewise, it is not well positioned to identify threats to system security by virtue of its isolation from these same authorities. CATSA authorities are cut off from higher-level public security agencies and are similarly cut off from security providers at the operational level. This is because its enabling legislation authorizes the delegation of responsibility for ground security operations to Local Airport Authorities (LAAs). These agencies, in turn, are permitted to contract services out to private security providers.

[22] *Canadian Air Transport Security Act S.C. 2002 c.9.*

[23] ACPA, 2001retrieved at: http://www.acpa.ca/newsroom.

Indeed, in the case of airborne security operations no one is in a position to coordinate such activities. This is because the legislation provides no formal channels capable of accommodating such initiatives.

The facts relating to both crashes provide insight into the threat from passengers checking bags containing explosives and then not boarding the aircraft. Solutions are varied and range in cost from relatively inexpensive to very costly. Hence, policymakers should make decisions on tried and tested risk analysis and risk management approaches.

Risk Analysis Approach

The classical definition of Risk Analysis is one that describes it as a process to ensure that the security controls for a system are fully commensurate with the risks. The Risk Assessment system should be simple enough to enable its use without necessitating particular security knowledge. This approach enables security to be driven into more areas and to become more evolved. Security should be properly targeted, and directly related to potential impacts, threats, and existing vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilities related decisions.

Quantitative Risk Analysis

This approach employs two fundamental elements: the probability of an event occurring and the likely loss should it occur. Quantitative risk analysis makes use of a single figure produced from these elements. This is called the "Annual Loss Expectancy (AE)" or the "Estimated annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated. Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

Qualitative Risk Analysis

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

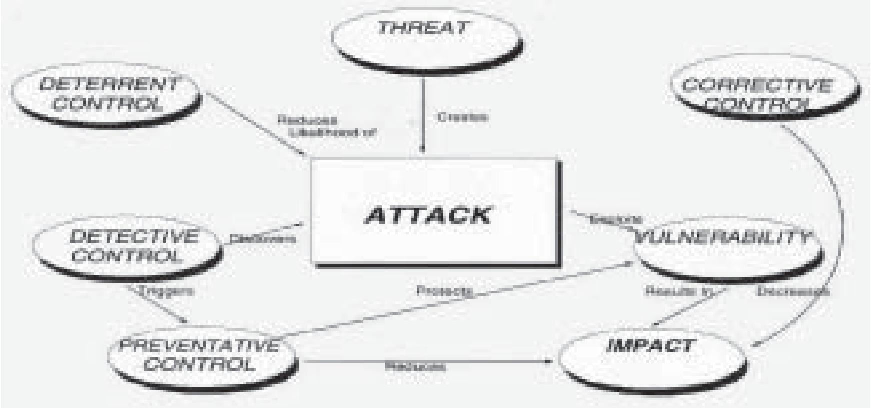
THREAT: These are things that can go wrong or that can ‘attack’ the system. Examples might include fire or fraud. Threats are always present for every system.

VULNERABILITIES: These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

CONTROLS: These are the countermeasures for vulnerabilities. There are four types:

1. Deterrent controls reduce the likelihood of a deliberate attack.
2. Preventive controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
3. Corrective controls reduce the effect of an attack.
4. Detective controls discover attacks and trigger preventive or corrective controls.

These elements can be illustrated by a simple traditional model:



[24]Sweet 2005

Tools in the Tool Box

The reminder of this paper will outline a number of countermeasures that can be used to respond to the dangers to aviation security revealed by the Air India and Lockerbie bombings and the methods of risk assessment

[24] Sweet. Kathleen. (2005). Transportation and Cargo Security, Upper Saddle River, NJ: Prentice Hall Publishers.

described above. One theme that will emerge is the appropriate mix of reliance on technology in screening passengers and their baggage in relation to reliance on human judgment and education. The tension between reliance on technology and judgment is underlined by the findings in the Rae report that those who used an explosive sniffer on the Air India baggage were inadequately trained and may not have had the appropriate equipment. A related theme will the relation between intelligence and interventions aimed at specific passengers and their baggage and interventions aimed at all passengers and their baggage.

A final theme that will emerge is how security improvements in one area such as passenger screening may make other areas such as the planting of weapons on planes by airport staff or placing bombs in baggage more attractive for terrorists and the need for a security system that accommodates for such substitution effects. For example, better screening of passengers and their baggage may also make it more attractive for terrorists to use should fired missiles or use mechanics or other airport staff to sabotage or place weapons on planes.

Passenger Profiling

A profile selectee or random passenger baggage match procedure is an interim solution that could be used until all airlines, to all destinations, could electronically track the passenger lists, boarding passengers and baggage on all flights. Such a system could also be utilized for cruise and rail passengers. The procedure has been the subject of much criticism. If a particular passenger meets the profile, or is selected at random, the passenger's bags receive additional screening both by x-ray and by an explosives detection system when available. This procedure unfortunately does not scan the terrorist who does not meet the profile or is not randomly selected.

A national database on passenger travel habits and history called the Computer Assisted Pre-Screening Passenger System or CAPPS was in use in the US. The original concept proposed a database based solely on travel information; however, it could later be cross referenced with FBI, CIA or criminal records, even though the FAA denies that this was being done. This system establishes some basis for risk assessment and does .indeed cut down the risk. At the same time, however, it also assumes that terrorist groups are not very bright and cannot escape the profile that attracts increased attention. Even though profiles are not published, parameters can be easily guessed. As stated, CAPPS II was highly criticized but should have been recognized, if properly controlled, as a valid tool in the security toolbox.

Passenger Protect Program/No Fly list

The proliferation of government watch lists are a troubling development in the "war on terrorism." The challenges of such lists include differences of opinion on who's actually a security threat, consolidating information across agencies by making the computer systems communicate the with one another. Canada's Auditor General Sheila Fraser found in 2004 that watch-lists used to screen visa applicants, refugee claimants and travelers seeking to enter Canada were in disarray because of inaccuracies and shoddy updating. [25]The challenge is complicated by the vast and growing databases of electronically stored personal information that draw on different agencies' records, which must be continually updated to be accurate. Agencies and airlines are using computer-driven algorithms to compare travelers' names against watch lists.

Use of Technology- X-Ray-Based Detection Systems
Standard X-Ray Scanners

Standard x-ray scanners have been extensively commercially developed and are available from a number of manufacturers. Units vary in cost, but quality devices range from $20,000 to $40,000 per unit. The standard airport hand-baggage scanner has a fan-shaped or scanning x-ray beam that is transmitted through the object to be viewed. The absorption of x-rays is usually measured by a line of detectors, and a high resolution image, derived from the degree of absorption of the beam, is produced. The image depends primarily on the density of objects located in the bag/cargo along the beam of the x-ray. These devices cannot distinguish between a thin sheet of a strong absorber, such as a metal and a thick slab of weak absorber. Simple x-ray systems rely on humans to serve as pattern recognition devices; in the absence of advanced computer pattern recognition techniques, they are very dependent on human factors. *This boils down to the proper training and competency of the screener.*

X-ray scanners are available in single and double monitor versions, with the two views being orthogonal. X-ray scanners can present images

[25] Auditor General's Report March 2004

in up to 80 shades of gray depending on the amount of absorption. Sometimes, the images are presented in a quasi-color where colors are used to produce an artificially enhanced visual presentation. Standard features now include image enhancement, automatic threat alert, full contrast and aspect stretch, high/low density penetration, sensor-free scrolling and automatic edge enhancement plus dual energy features with organic and inorganic stripping displayed on two monitors.

Dual- or Multi-energy Scanners

These devices have also become commercially well developed by several vendors**.** They are available at approximately $100,000 per unit. These dual energy systems are actually comprised of two separate x-ray systems whose beams are generated by sources that peak at different energies, producing two independent images. This higher energy view requires less absorption. While areas of heavy elements are dark in both views, areas of light elements are darker in the lower energy projection. By comparing the two images, light elements such as carbon, nitrogen and oxygen may be highlighted. In this way, it is possible to determine whether a given object is made of a light or heavy element. Multi-energy systems are essentially the same except that they have a single x-ray tube that transmits a broad spectrum of energies. Detectors are used to select specific energy regions. These systems then combine to produce effectively the equivalent result.

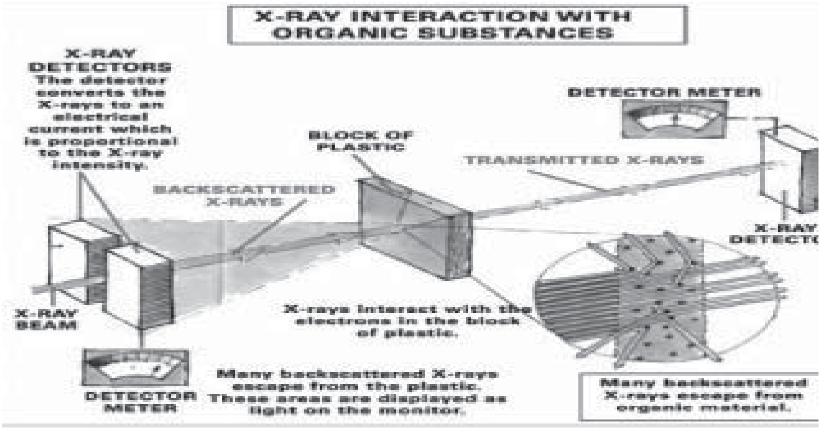
This technique cannot distinguish among the light elements. However, it can overcome the countermeasure of hiding explosives behind an object made of a heavy element, unless enough material is present to absorb the entire beam, which would require an 8-10 mm piece of steel. (I.e. can you hide explosives behind a heavy object with a regular x ray machine discussed above)? These devices are technically identical to a simple x-ray scanner, except for the dual energy and image feature. The systems use color to separate the image into organic, inorganic and opaque materials. The organic consist primarily of light elements, the inorganic of heavy elements and the opaque materials, which would contain a lot of heavy element matter. Explosive materials are made of organic matter and some scanners assign the color orange to organic materials in order to make them more clearly visible.

Backscatter X-Rays

Backscatter X-rays are also commercially available and use computer algorithms to function in order to automatically detect explosives. Systems are available from between $60,000 to $100,000 per unit either as a single or dual viewing system. Most systems scan a pencil beam of x-ray across the object and create two images: the normal transmission image, created by a single detector on the opposite side and a backscatter image, created by a large area detector on the side of the entering beam. A single energy beam is utilized. A two-sided version of this system with two identical x-ray beam systems makes backscatter measurements from opposite sides of the object to enhance the backscatter penetration of the system. The transmitted beam provides a typical x-ray image showing primarily the absorption by heavy elements. Backscatter signal intensity depends on how much of the transmitted beam has been absorbed, how much is backscattered and how many of the backscattered x-rays reach the backscatter detectors. The backscatter signal depends on the competition between photoelectric absorption and Compton scattering. The photoelectric cross section increases with the atomic number of the object, while the Compton cross section is relatively independent of atomic numbers. The resulting backscatter signal favors the low elements with particular emphasis on low elements of high density, including plastic explosives. Backscatter imaging provides a direct measure of the density of elements with low atomic number.

Most manufacturers produce two independent x-ray images: an x-ray transmission image emphasizing the high elements and an x-ray backscatter image emphasizing the low elements. Systems are unique and utilize proprietary techniques.

Companies continue to research a computer algorithm for automatic detection of explosives with the aim of achieving a high probability of detection and a low false alarm rate for explosives. The automatic detection scheme is based on an algorithm that compares properties of bag images against acceptable thresholds. The system builds a database of acceptable histograms by observing and “learning” the characteristics of a large variety of luggage. An algorithm sorts and combines data for online comparison with acceptable values.


X-RAY INTERACTION WITH ORGANIC SUBSTANCES
X-RAY DETECTORS The detector converts the X-rays to an electrical current which is proportional to the X-ray intensity.
BLOCK OF PLASTIC
DETECTOR METER
TRANSMITTED X-RAYS
BACKSCATTERED X-RAYS
X-RAY DETECTO
X-RAY BEAM
X-rays interact with the electrons in the block of plastic.
DETECTOR METER
Many backscattered X-rays escape from the plastic. These areas are displayed as light on the monitor.
Many backscattered X-rays escape from organic material.

[26].

Another device produces a virtually "naked" image of passengers by bouncing x-rays off their skin. The device however does enable staff to instantly detect any hidden weapons or explosives. A test program started in (2004) is still underway at London's Heathrow Airport, Terminal 4. As discovered previously during a test at Orlando Airport in Florida in 2002, the graphic nature of the black and white images has raised some concern about the privacy of passengers. In the US, the deployment of such equipment has been delayed until the developer can refine a method to mask the passenger's modesty. At Terminal 4 in London, the trial is being conducted jointly by British Airports Authority and the Department of Transportation.

If the body scanner is able to cope with large volumes of travelers, improves detection and receives public acceptance, it will likely be deployed throughout Britain. Passengers are currently selected to go through the body scanner on a random and voluntary basis. Those who decline are subjected to hand search. The scanner resembles a large filing cabinet and is operated in a curtained area. Once screened, the images are automatically deleted. Security officials are pleased with its effectiveness because it detects the outline of any solid object, which conventional metal detectors might be likely to miss. Managers are citing the positive aspects of the ability to avoid intrusive hand searches. Regardless of its effectiveness, passengers are still a bit startled by the clarity of the image. This technology as application for passengers and bags.

[26] Electronic Privacy Information Center, Transportation Agency's Plan to X-ray Traveler's Should be stripped of Funding. (June 2005) Retrieved from: http://www.epic.org/privacy/surveillance/spotlight/0605/

Computerized Tomography (CT) (Baggage only)

This system represents an adaptation of a compact, fast and mobile medical CT scanner. The main difference between the two types of use (security at airports and medical diagnosis) is that the machines used in transportation facilities have more shielding to stop the scattered radiation where, in medicine, the patient is not shielded. The concept utilizes a conventional x-ray scan projection to locate areas with sufficient density to represent a possible threat. In addition, multiple detectors placed on a rotating circumferential element around the object, measure the transmitted signal from a fan beam that traverses it. The density at each location along the path of the beam can be determined, with the rotating action giving the information to provide a complete two-dimensional slice. The inspected object is moved through the detector beam by means of a conveyer belt, providing the third dimension i.e. multiple slices then creates a computer projection with good spatial resolution.

The system operates and looks like a medical scanner or medical CAT computerized axial tomography scanner. The explosive detection device was adapted based on the same principles. The system first produces an x-ray scan similar to the conventional x-ray scanner**.** An automated inspection algorithm determines the locations within the baggage where the absorption indicates a suspicious area; cross-section CT slices then need to be made to determine the density, texture, mass and shape of the object. Dual-energy CT, a theoretically possible, although not yet implemented option, would also provide information on the nature of the explosive. If no high-density areas are detected, a single slice through the bag is made to look for any sheet explosives that may not have been seen in the projection scan. Since the CT scan produces true cross sectional slices, it is able to identify objects that are surrounded by other materials or hidden by innocuous objects. When alarms are encountered, the CT Scan operator can make further slices to reveal size, shape, mass and make-up of the suspect object. Three dimensional rendering may also be applied.

Trace Detection

Trace detection may be best known for its explosives detection capabilities. Trace detection refers to a group of products that can analyze a swipe or air sample, detecting and identifying minute traces of substances. Some equipment can access the human convection plume, a natural airflow phenomenon radiating from the human body, to collect any threatening particles. The plume moves upward and predetermined flow rates help the hood capture optimal information. If someone has explosives strapped to their bodies or has even handled explosives, those trace particles will contaminate clothing and register. The machine uses the plume as the vehicle to capture the sample and send it to the detector hood.

The process takes four seconds to collect the trace particles and another 8 seconds to analyze it. A proximity sensor activates both visual and audio prompters for the passenger to enter. As the person stands in the center of the archway, gradually stronger puffs of air come from four surrounding columns positioned to direct them from the lower to the upper body parts of the body, accelerating the plume at a faster rate than it would naturally rise. The plume is collected in the overhead detector and collected particles are vaporized. The molecules are either positively or negatively charged to become ions, which are pulsed down a drift tube. The equipment measures in milliseconds how fast the ions travel from point to point. This acts as the thumb print of the substance, since each specific type of ion has its own particular travel time. This enables the machine to identify a broad range of organic matter, including explosives. The systems also perform high speed baggage inspection to accurately measure mass, density, atomic number and other physical characteristics of objects, providing three independent x-ray images of each bag. Using algorithms software, the MVT can pinpoint the direct location of suspect items to decrease the time length of the search. The MTV's belt speed of 100 feet per second scans 1800 bags per hour, as opposed to airport screeners that process bags at a rate of 400-500 per hour. The MTV is approximately three times cheaper than current scanners, costing about $500,000 per unit. As regards the Ion Track Itemiser, it uses ion trap mobility spectrometry (ITMS®) technology. It is extremely simple to use. The surfaces of a vehicle or luggage that are suspected of being tainted with contraband are wiped down with a paper disk known as a sample trap. The trap is then inserted into the desktop analyzer. Once analyzed, the contraband substance is identified, along with its relative alarm strength. Visual and audible indications are provided, and the analysis can be stored and printed for later use as court-accepted evidence.

In late October 2004, the TSA deployed an explosive detection trace portal from Smiths Detection of Pine Brook, N.J. at JFK International Airport in Terminal One. It was to remain deployed for at least 90 days during the pilot program. Rear Admiral David M. Stone, Assistant Secretary of Homeland Security for TSA used the deployment as means to reiterate that the TSA is committed to using cutting edge technology. The passenger walks through portals similar to metal detectors. Puffs of air are blown at passengers and samples are then collected and analyzed for explosives. If the portal's alarm sounds, the passenger and or property are screened more intensely. This type of machine had already been deployed at T.F. Green State Airport, Providence, R.I., Greater Rochester International Airport, San Diego International Airport, Tampa Florida International Airport and Gulfport Biloxi International Airport.

On 22 September 2004, the TSA also announced the deployment of some related technology. They deployed a new Explosives Trace Detection Document Scanner that can "sniff" passenger documents such as boarding passes and drivers' licenses for traces of explosives at several major airports. The airports are Los Angeles International (LAX), New York's John F. Kennedy (JFK) and Chicago's O'Hare International (ORD)."TSA is committed to deploying new explosives detection technologies to passenger security checkpoints to safeguard the traveling public," said Rear Admiral David M. Stone, USN (Ret.), Assistant Secretary of Homeland Security for TSA. "TSA continues to lead the way in utilizing the latest emerging technologies with various pilots to screen both passengers and air cargo for explosives." [27] The pilot program was first unveiled, a few weeks prior, at Ronald Reagan Washington National Airport. Tests were conducted for a minimum of 30 days at each airport. The Document Scanner analyzes samples collected by swiping the surface of a document over a collection disc and alerts the screener if explosives residue is detected. During the pilot, passengers selected for secondary screening at particular checkpoints had their boarding passes scanned. If the Document Scanner alarms, additional screening procedures are implemented. This pilot is one in a series of next-generation tools being tested by TSA including explosives trace detection portals, which are being tested in four airports with nearly a dozen more to come online in the near future.

Quadruple Resonance

Quadruple resonance uses carefully tuned pulses of low intensity radio waves that probe the molecular structure of targeted items, such as

[27] TSA News Release, http://www.tsa.gov/ public/ display?theme= 44& content =09000519800cf9c8

explosives or narcotics. The waves momentarily disrupt the alignment of targeted nuclei, which produces a characteristic signal picked up by a receiver and sent to a computer for rapid analysis. "The signal emitted by the explosive or drug is unique," says Lowell J. Burnett, president and CEO of Quantum Magnetics Inc., a subsidiary of InVision. "Specialized radio frequency pulse sequences have been developed for the optimal detection of such explosives as Semtex, C-4, Detasheet, TNT, tetryl, ANFO, and black powder, and such narcotics as cocaine or heroin."

Metal Detectors

Previously, passengers were required to pass through simple metal detectors before boarding a vessel or aircraft or entering a facility or sterile concourse. However, such efforts have been repeatedly found to be less than 100% effective. There are still easily recognizable deficiencies in many current metal detectors. They simply do not trap all forms of dangerous weapons. More often, their greatest weakness is often cited as the inability to detect metals incapable of being magnetized. Since a significant number of US manufactured guns are made of nonferrous metals, the shortfall is quite evident. They also can not detect the organic materials contained in explosives. Regardless, metal detectors remain one of the most important sources of security for transportation facilities. Additionally, there have been significant advances in equipment which include software programs that can suppress ferrous detection while boosting non-ferrous metals. Others suppress non-ferrous materials while magnifying the detection response of ferrous objects.

The scientific principle upon which metal detectors work is quite simple. Passive systems detect metal by changes in the earth's magnetic field. Active detectors operate by creating an electro magnetic field and alarming when the field is disturbed by metal objects passing through it. Metal detectors contain one or more inductor coils that are used to interact with metallic elements on the ground. A pulsating current is applied to an internal coil, which then induces a magnetic field. When the magnetic field of the coil moves across metal, the field induces electric currents called eddy currents. The eddy currents induce a magnetic field which generates an opposite reaction in the coil, which induces a signal indicating the presence of metal. [28] Standard features now include improved target discrimination, increased throughput traffic

[28] "How a Metal Detector Works", http://micro.magnet.fsu.edu/electromag/java/detector/ pg 1. 24 July 01.

flow, advanced signal processing, lower false alarm rates and higher threat object detection rates. Regardless, problems have continued even in the use of these relatively simple machines. For example, in 2002, for the second time in a three year period, a metal detector was accidentally unplugged at Logan International Airport, triggering a security breach that prompted the evacuation of 750 passengers and delayed 11 flights.

Selecting a Metal Detector

The selection of an appropriate metal detector is an important decision to be made by transportation facility and mode of transportation officials. Each facility has its own unique characteristics and priorities. Unfortunately, one of the primary limitations is usually cost and metal detectors can be expensive assets that need maintained and routinely upgraded.

Additionally, the accuracy and utility in the passenger environment of each detector is a weighty aspect. The growing demand for security at access points has moved technology toward walk-through and hand-held metal detectors. The rapid flow of passengers is of major concern to airlines seeking to keep their balance sheets on the positive side of the ledger. In order to keep on making money, the various components must keep the passenger relatively agreeable to the delays caused by screening 100% of the terminal or station traffic. Equipment causing too many false alarms, breaking down on a repeated basis or otherwise causing delays is not marketable in these venues.

In order to satisfy market demand, many companies have been through innumerable successive generations of equipment. Those improvements have featured increased levels of security performance in metal detection capability, discrimination of personal metal objects, and immunity to outside interference. Safety precautions regarding the passenger with a life support device have also been tested and re-tested to protect the operator and manufacturer from civil liability.

Of course, the bottom line for each metal detector is whether or not it actually accurately detects guns and dangerous weapons. The actual detection rates are for security reasons not published. Suffice it to say they must possess a high detection rate. Today's hardware and software programs improve interference rejection, discrimination, sensitivity, detection, uniformity, vibration tolerance and orientation response. All of these factors contribute to the bottom line that increased discrimination significantly reduces unwarranted alarms. Many metal detector manufacturers now also sell enhancement programs that help correct detection non-uniformity caused by vertically positioned external metal. Other programs allow the user to create customized security programs. Additionally, the proficiency of the operator is also a critical factor.

The manager circumnavigating the hundreds of pages of marketing materials on metal detectors still has to consider some basic concepts in determining the most appropriate system for their particular use. Overall, managers need to contemplate such issues as external factors or sensitivity to environmental factors (i.e. environmental magnetic noise); Physical construction or size; Ease of Operation, (i.e. ease of calibration, self calibration, and required frequency of calibration) and last but not least cost and appearance.

Additionally, development has produced machines, which now have a multi-zone advantage. In addition to indicating the location of targeted objects, multi-zone systems have a multitude of advantages. They improve discrimination between weapons and harmless objects, reduce unwanted alarms and permit higher traffic flow rates. In high volume airports this translates into lower operating and capital costs. For example, pin-point multi-zone detection is a concept formerly pioneered by Ranger. The manufacturer uses a "block of real estate" example to explain the dynamics of the system. They explain that in "most detectors the blocks of real estate, called zones, are stacked upon each other and extend the full width of the archway. When an object passes through a zone, it is detected by the zone and an alarm display shows its location. In this case, the alarm display depicts the height of the object above ground. The display can take the form of lights on the front edge of a side panel or a mimic display that represents the archway in graphic form."[29]Manufacturers do place different interpretations on the meaning of multi-zone detection. Appropriately, when a device claims to have 6 horizontal zones, it should mean that there are twelve detection channels with two sensors per zone. Each zone should be independently adjustable.

False alarms are attributable to external electrical and electro-magnetic interference and poor tolerance vibration. Good quality interference

[29] Defining Multi-Zone Detection: Check Apple for Apples", http://www.omni-security.com/wthru2/wtindex.html, pg. 2, 3 May 2001

rejection and mechanical design will lower false alarms. Multi-zone detectors reduce unwanted alarms caused by people literally wearing metal; jewelry, coins, keys etc. Two conditions contribute to elevated undesired alarm rates. They include the cumulative signal effect and non-uniform detection. Cumulative signal effect lowers a detector's ability to separate weapons from harmless personal effects. It occurs when signals generated by metal are processed as a single composite signal. Theoretically, in single zone machines, the signals from someone's watch, their keys and some metal in their shoe will be combined. If the cumulative signal is large enough, the machine will alarm causing delay and frustration for passenger and screener alike.

Correspondingly in multi-zone detectors, if the device has 18 zone detectors, six horizontal zones would be divided into three blocks. The machine would then display the object's height above the ground, and also show if the object was to the right or left or in the center of the zone. Complicated mapping algorithms process the data and can very accurately tell the scanner where the object is. Because each zone has an adjustable control, the sensitivity can be focused and a particular object for a better analysis thereby making a threat assessment easier and reducing unwarranted alarms.

Another feature to consider before purchasing a specific piece of equipment is the information the screener receives from the alarm panel during an alarm. The alarm panel should show the height at which the detected object is carried. For example, more advertised zones are not necessarily better unless the numbers of horizontal sensitivity controls are present to adjust those zones. This is arguably more important than the actual number of zones. This significantly cuts down on the time needed to actually locate a weapon if there is one. Furthermore, the equipment should be continuously active, have self-testing diagnostics and a fast automatic reset. Electrical and electro-magnetic interference rejection can be achieved through multiple frequency selection, electronic filtering and sophisticated software algorithms.

Hand Held Body Scanners

The best hand held detectors are light weight in construction, have a comfortable grip and a large scanning surface. The detector should have a tight detection pattern, fast detection circuitry and be ergonomically designed. These attributes contribute to higher efficiency and reduced operator fatigue. Another really useful feature is a switch which can transform the detector from a general use mode to a super high sensitivity unit capable of detecting very small masses of metal.

They should generally have been able to detect a Medium pistol at 12 "(300mm); a Small pistol at 9" (230); and a Razor Blade at 3" (25m) and should scan about 3" to 24" per second. They also need to be adjustable. For example, the controls should enable to the scanner to lower the sensitivity to avoid unwanted alarms for small harmless objects like key chains. Sensitivity adjustments are usually made through a screwdriver access hole in the handle. Most quality devices encase the circuitry in a rugged high impact case which should detect both ferrous and non ferrous metals and alloys. It should be capable of not alarming when the scanner is used to screen at ankle height and in the vicinity of re bars in the floor.

Alarms are both visual and audio. They should remain activated while the search coil is over a metal object. The duration of the alarm is usually indicative of the size of the object. Most use alkaline batteries in a power source which should last at least 80 hours. Low voltage conditions, like cell phones, should advise the user that the power is low. The average weight is a pound or less. Visual only alarm indications are advisable if a weapon is detected. The screener can simply ask the individual to step to the side for the moment, giving security personnel time to respond accordingly. An audio alarm also alerts the perpetrator that they are "trapped" and they may respond accordingly. Generally**,** as stated no more than 15% of the people who alarm the detector should be false alarms. In other words, no more than 15 unarmed passengers out of 100 should alarm the detector.

Interim Conclusion: Equipment

Screening of passengers and their baggage on all sorts of modes of transportation, in conjunction hopefully with future cargo screening, will continue way into the 21st Century. How intrusive the measures can become before the public rejects the level of intrusion will be dependent upon the threat as it is perceived by the traveling public and not necessarily the government. Technological advances continue to be made and improvements in technology will equate to improvements in security. The better the equipment the more reliable the results, as long as the supervisors of screeners train them appropriately.

It is an international offense to "knowingly and willfully" enter an aircraft or airport area in violation of security requirements and yet millions of people try it. So called security experts even boast what they carry on in a concealed manner; trying to make the whole process into a joke. Such conduct, misconduct if you will, exhibits unprofessional conduct and does not further the safety and security of the traveling public. The penalty for having weapons in a secure area is stiff and include up to 10 years in prison, with or without a separate fine especially if the prosecution can prove you intended to commit a felony, like hijacking. It is possible to receive a sentence of a year imprisonment simply for breaching security. If an individual is apprehended actually carrying a weapon onto a vessel, similar to the British journalist who smuggled a meat cleaver and a dagger onboard a flight out of London's Heathrow Airport, it is possible under UK and US law to be imprisoned for 10 years to life.

The CATSA/TSA systems have been plagued with the same problems as the former private security companies that manned the machines. They were supposed to put safety first. That is, they were not supposed to put passenger convenience and flight schedules ahead of security. Such was the primary reason why legislators had "federalized" the airport-screening workforce and created the new agencies in the weeks after the September 11 attacks. No longer would airport security be left to minimum-wage workers, employed by and answerable to the airlines.

But after five years and billions of dollars, former and current screeners from numerous airports around North America continue to report that procedures are routinely violated to accommodate the airports' and airlines' business needs. According to the screeners, luggage is often loaded onto planes without being screened for explosives, and passenger checkpoints are regularly understaffed, increasing the risk of guns and knives being smuggled aboard. The bottom line, they say, is that screeners, under pressure from the airlines, has loosened its security practices to eliminate hassles for passengers and, in doing so, has seriously compromised safety. If this is true, all the technological improvements in the world will not improve security at transportation facilities.

The transition process for security operations since September 11, 2001 has not been smooth, but much progress has been made. However, transportation security is still a "work in process." New technologies being developed will significantly affect many of the operations in place today Depending on the changing nature of system threats and the tolerance of the public to intrusion levels, transportation security equipment will continue to evolve. Cargo screening in particular will be improved. In fact, it must be or a similar catastrophic event might occur similar to the Air India or Lockerbie tragedy or worse.

Bomb Sniffing Dogs

Dogs have a great sense of smell. Their noses are about 100,000 to a million times more sensitive than a human's nose and a well-trained dog can detect up to 20 different kinds of explosives. Furthermore, the legality of their use is well established and do not seem to be significantly limited by civil liberty type legislation. Dogs disclose only the presence or absence of illicit substances and nothing more. They are less intrusive than a typical search and the limited disclosure exposed the property owner to a minimum amount of inconvenience.

Canines are also less expensive than other means of explosive detection. Dogs costs about $6000 to train and a piece of equipment can cost more than a million dollars. Currently, dogs are generally only used at airports if the threat of a bomb is eminent. Bomb sniffing dogs are not without their problems, which include short attention spans, false alarms, sickness, and distraction of female dogs in heat. To pass the normal certification test, the dogs must receive a score of 100% accuracy. They must convince the handlers that they can successfully detect at least 20 known explosive compounds, which enables them to identify over 19,000 varied explosive combinations. Their training system is based on a food reward program. The method rewards the dog for detecting a compound. To re-enforce the conditioning, they are never fed without some exposure to an explosives' odor. This keeps the dogs highly motivated to sniff out the explosive, because food is always available if they do. The ATF and the US Department of State have provided dogs and training to numerous airport authorities around the world. The program was successfully used by the Australians before the 2000 Olympic Games and has been in operation at high threat airports for a number of years. Dogs are compact, mobile and capable of working in a variety of environments including confined spaces. More importantly in the airport environment they can reduce the manpower needed to screen huge quantities of cargo.

Hiring and Good Management

Hiring, normally within the purview of a department of human resources, is actually the most critical element in establishing a good security program.

All references should be checked and all educational qualifications should be confirmed. Candidates should also sign a document swearing to the fact that they have never been convicted of a felony. As confirmation of the truth of that statement, criminal background and history checks should be conducted through local, state, federal and international authorities where suitable. It is also recommended that psychological examinations be utilized. Additionally, it is very important that human resources administer tests certifying each candidate possesses adequate communication skills to include the basic ability to communicate verbally and in writing in an appropriate language prior to hiring. Previous employment history should be verified as well as actual contact made with all listed references. Lastly, pre employment and regular drug screening procedures need to be a mainstay of the program. These basic hiring criteria are even more critical if the security officers are to be armed during the course of employment. All initial hires should be advised of a discretionary probationary period during which they can be dismissed for any reason.

Indoctrination

Exposure to the CATSA philosophy and mission is important but even more so is a security awareness attitude that is instilled into the new employee from the very first day of employment. Standards of minimum acceptable conduct must be supplied to the employee and they should sign a document indicating they understand those standards. The employees should also be made aware of the uniqueness of working within the transportation system milieu and the potential consequences of a lapse in security. Other standard orientation subjects should include thorough instruction in procedures and policies, emergency response techniques, report writing, legal authority and familiarity with equipment usage.

As mentioned, the employee should be briefed on the utilization of a random drug screening program and that they are subject to testing on a constant basis. They should be made aware of the fact that failure of such a test will result in loss of employment. A drug rehabilitation program is not an appropriate alternative to employees within a security function. Another disqualifier is for new employees to fail the training provided during orientation. Unsuitable candidates can usually be easily identified and replaced before being placed in the work setting. Officers should be able to review the facilities overall master security plan. Additionally, a security manual with a set of operational instructions (IO) should exist and be reviewed. Compliance with the IO's should result in adequate security for the facility with specific responsibilities clearly detailed.

Training

Employee training should always contain immediate advisement of the objectives of the training. Employees should know what body of knowledge they are expected to retain upon completion of the training. Training which does not conclude with a test often leads to a lax attitude toward the training. The ultimate goal of training is higher job performance on the job. Non retention of the material nullifies the period of instruction and is a waste of employee paid time. Furthermore, a trained officer is much less likely to make errors which could result in a loss.

The question of whether to train staff in situ or send them to an off site training course is always a determination of cost, availability and quality. Off site courses may or may not coincide with facilities schedules and or budget. If on-site training is chosen, the instructors should be certified and competent.

Access Control

Access control restricts the ability of unauthorized individuals from gaining access to a specific area. Access control systems assure the proper identification of personnel across multiple facilities and locations on a selective basis, to secure areas. In 1000 BC the Chinese required servants at the Imperial Palace to wear rings engraved with unique intricate designs identifying palace areas they were permitted to enter. Historians credit this method by the Chinese as the first comprehensive access control system. [30] Advancement in science and technology has improved on the Chinese system. Some systems can also be programmed to lock and unlock access points at specific times and on specific days.

The best equipment should also maintain detailed records of movement through secured areas. The coded information can record time of access, zone accessed and duration of access. There are two basic types of access control devices- the card reader and the code transmitter. These devices read magnetically coded information on a card or a small transmitter emitting a continuous signal which is worn by the user. The information

[30] John Naudts, "Access Control; It's in the Cards", Security Management, 1987, pg 169

is transferred to a computer that compares the received information with a database. If the information does not match, the system can be programmed to alarm. Computers have brought much more sophisticated approaches to access control systems.

To keep official documents, uniforms and vehicles out of the hands of terrorists, most security experts suggest the following protective measures:

Keep comprehensive records of all official identification cards, badges, decals, uniforms and license plates distributed, documenting any anomalies and canceling access for items that are lost or stolen.

Practice accountability of all vehicles to include tracking vehicles that are in service, in repair status, or sent to salvage.
Safeguard uniforms, patches, badges, ID cards, and other forms of official identification to protect against unauthorized access to facilities, to include stripping all decommissioned vehicles slated for resale and/or salvage of all agency identifying markings and emergency warning devices.

Check multiple forms of valid identification for each facility visitor.

Verify the legitimate business needs of all approaching vehicles and personnel.

Improve identification card technology to eliminate reuse or unauthorized duplication.

Alert uniform store vendors of the need to establish and verify the identities of individuals seeking to purchase uniform articles.

Ensure all personnel are provided a security briefing regarding present and emerging threats.

Encourage personnel to be alert and to immediately report any situation that appears to constitute a threat or suspicious activity.

Arrange for law enforcement vehicles to be parked near entrances and exits.

Limit the number of access points and strictly enforce access control procedures.

Institute a robust vehicle identification program, including but not limited to checking under the undercarriage of vehicles, under the hood, and in the trunk.

Provide vehicle inspection training to security personnel. [31]

Computers have revolutionized access control systems. The use of voice recognition systems, signature recognition, retina recognition, hand geometry and fingerprint recognition has all expended biometric technology to be a cost effective and highly accurate alternative to cards.
All aviation related systems should require that access control systems must:

1. Enable only those persons authorized to have access to secured areas to obtain that access.
2. Immediately deny access at the access point to individual's whose access authority has changed.
3. Have the capability of zone coding, so that it can admit or deny access by area.
4. Have the capability of time-coding, being able to admit or deny access by time and date.

Barriers

The primary function of a barrier is to delay the intruder as much as possible and to force him to use methods of attack that are more conspicuous and noisy. As the value of the target increases, however, the strength of the barrier must increase proportionately. The trade-off between delay time and detection time is perhaps the single most important consideration in designing a barrier. Some facilities are protected by a natural barrier, such as the water surrounding Alcatraz. Usually, however, a barrier must be constructed as a physical and psychological deterrent to intruders. Fences, define the site perimeter, briefly delay an intruder, channel employees and visitors to authorized gates, keep honest people out and serve as a sensor platform. Barriers such as a chain link fence have the

[31] Retrieved from : http://www.identicard.com.

added advantage of being able to see through it, where solid walls block security's view and the intruders view.

Perimeter barriers, according to the NCPI are, "any obstacle which defines the physical limits of a controlled area and impedes or restricts entry into the area. It is the first line of defense against intrusion… At a minimum a good perimeter barrier should discourage an impulsive attacker." [32]

Smart Cards

Today, Optical Memory Cards and smart card technology is the way of the future. They possess one or more integrated circuit chips capable of storing a great deal of information and interpreting it. Each card must authenticate identity and contain a photograph and microchip when the holder logs onto a computer or enters a facility. However, smart cards are very complicated entities. It is just this complexity which might doom them in the market place. They require sophisticated microprocessors and exhaustive authorization procedures. An even newer technology might replace them.

None of these cards provide effective security in the wrong hands. The card does not know who is holding it and the machine reading the signal or data does not know either. An access card can simply not identify a specific individual using the card. It is only wishful thinking to assume that every time a card is used that the person using it is actually the person authorized to use it. As mentioned previously, piggy backing is also a problem. One person opens the door or access point and several people follow them through. Another issue arises when terminated employees fail to turn in their security badges, but some companies are attempting to rectify this problem with cards that expire.

Biometrics

Employees should all need to enroll their fingerprints or some other unique physical trait into a database. Biometrics have progressed a long way since the first models appeared on the commercial market. The information stored in biometric system databases are usually the name, ID pass number and the fingerprint or other trait of the employee into a template. The process of enrollment takes about 5 minutes. The employee

[32] National Crime Prevention Institute, *Understanding Crime Prevention*, Stoneham, MA., Butterworth Publishers, 1986)

can access restricted zones by presenting their ID cards to a proximity reader which acknowledges the employees ID number. They then place their finger, hand, retina or face onto or near the biometric scanner. A signal is sent from the scanner to the biometric database, requesting that it reconcile the badge number with the imprint. In the matter of two seconds the equipment recognizes the employee and displays green or rejects the possible intruder. International biometric standards are currently being developed.

Access to the database must be restricted to designated personnel and must be inaccessible outside the facilities network. Biometric information must be encrypted. Systems will not only improve the level of access control but will also reduce the risk of identity fraud while increasing confidence in security. Generally, biometric systems are designed to recognize biological features of individuals in order to facilitate identity verification. There only drawback is that in today's modern medical world, physical characteristics can be changed. Currently, the following types are available commercially.

a. Fingerprint- optical scanning of a finger which is matched to a database.

b. Signature recognition- relies on the fact that individuals write with distinct motion and pressure. Forgers can duplicate the appearance but not the style.

c. Hand geometry- utilizes the physical attributes of the hand such as the length of fingers.

d. Speaker verification- utilizes the uniqueness of voice patterns.

e. Eye retina- analyzes the blood vessel pattern of the retina.

Closed Circuit Television CCTV

Closed circuit television has become the most common security device in many applications, not just along a perimeter. Their sophistication may range from simple fixed black and white monitoring cameras to infrared capability. They can be used in corridors, entrances and secured areas to name just a few. Cameras can instantly monitor activity near a fence and record the intruder if needed. Some are even equipped with motion detectors to alert a guard that a camera has detected an individual near the fence. They have become indispensable in today's security world and come in all shapes, sizes and budget requirements. A significant enhancement to CCTV came with digitization. For example, now a QUAD can compress images from four cameras into a single frame of VCR tape or DVD, allowing the operator to view all four cameras on a four way split screen. Video multipliers also allow the system high speed, full frame recording from multiple sources. Infrared cameras now also can be used for night surveillance. Newer systems provide sharp images of distant subjects at high frame rates with remarkably reliable recording apparatus. The number of cameras one officer can control is theoretically unlimited but in reality, the more cameras the less time spent on each view. The International Professional Security Association Security Instruction and Guidance Manual recommend the following:

Sequential switching- fixed cameras are sequentially switched to a single monitor and the operator has a view of each location in turn.

Motion switching – a fixed camera that covers a static scene can be made to switch to the monitor if any movement is detected by the lens.

Combination- the sequential switching is interrupted if a camera detects some motion within the field of view and the image is presented on the screen.
Manual control- the operator is able to switch each camera into the monitor screen as required.

Multi-screen- several small screens simultaneously display the images from the various cameras: used where the cameras are rotated, tilted, zoomed, etc. by the operator. Often a picture of interest can be switched to a larger screen for detailed examination. The quality of recorded images must be very high so that people, objects and vehicles can be identified. Highest quality is required especially when the subject occupies only a small fraction of the camera field of view because the image must be enlarged to see the subject. Images require not only high numbers of pixels, i.e. the full native resolution of high quality, CCTV cameras, but also have high sharpness and few compression artifacts. For this, high data rates are needed unless the frame rate is extremely low, but a low frame rate reduces the chance the subject is video photographed facing the camera and that no objects block the view.

Improved capture of the images of moving objects is needed since transportation platforms or passengers are often moving. Video cameras should have progressive scan, rather than the common interlaced scan of broadcast TV. The problem is that cameras with interlaced scan require two interdigitated snapshots for each full-frame image, one for the even scan lines and one for the odd scan lines. Subjects often move during the time that elapses form the first half of snapshot to the next, blurring the combined image. The use of progressive scan rather than interlaced scan often gives the increased sharpness equivalent to an exposure period that is reduced by ten-fold for a subject that occupies a fraction of the height of the image.

The video security system for transportation systems should be able to do a first level of screening of the video captured in real time to reduce the amount of manpower required to identify potential threats. The motion detection algorithms used in stationary systems, where the camera is affixed to the wall of the building are not adequate because the only motion is motion of potential subjects, not motion of the platform, i.e. motion of a train or ship, and thus movement of the camera. It must be possible to communicate live images in real time from both mobile and fixed platforms to security personnel who are stationed on them. Requiring the use of only powerful desktop and notebook computers with a high-speed local area network is too restrictive a requirement for viewing live and recorded images from multiple cameras simultaneously.

Finally, since video, access control, biometric and other sensor systems must be integrated together to form a total security solution, the video security system should be designed so that it can easily be integrated into other systems.

Alarms

Should the fence, barrier or wall be circumvented, alarm systems are the next line of defense. Alarms can be silent, audible or visual. Visual alarms are specifically designed to catch someone's attention to a potential problem. A blinking red light is the classic example, either on a control panel console or at the site of the alarm involved. Audible alarms are intended not only to alert security but also to scare the intruder. Silent devices are designed to alert security as well as law enforcement if desired.

Lighting

Adequate lighting on the perimeter is also a mandatory security function. The spread of the light should be directed outward from the fence line. This will illuminate the approach of an intruder and also obstruct the intruder's view. If closed circuit television is part of the perimeter protection scheme, the placement of the cameras and lights must be coordinated. Careful attention should be paid to not creating areas of shadow and glare; preventing an unobstructed view.

An Integrated System of Access Control

The number of gates providing access should be limited to the number of essentially required entry points. Gates either need to be guarded by security officer or constantly viewed by some sort of electronic equipment, either CCTV or by use of a card actuation system to gain access. Earlier methods involved simply padlocking the gate and providing keys to only those truly needing them. Advances in technology enable security now to utilize electronically generated controls, key card access, keypad access and others depending on the budget of the operation. Dogs are also a viable option.

A fence provides minimal protection. Lighting adds to the protection level. However, the combination of a fence, proper lighting, and at least two sensors greatly increases the probability that an intruder will be detected. Sensors can be expensive, and the actual threat must be weighed against the cost. Sensors in alarm systems range from simple magnetic switches to sophisticated Doppler radar. Alarm systems vary but all have three basic common elements.

A. an alarm sensor

B. a circuit or sending device

C. an enunciator or sounding device

In choosing a system, the object, space or perimeter to be protected is the very first consideration after which an analysis of the intensity and frequency of outside noise, movement or potential interference must be factored into a final decision.

Summary

Most countries have taken a "legal" or "criminal" approach to prosecuting terrorists. They assess the results of an attack and pursue a public legal remedy based on the specific misconduct already deemed criminal in a standard penal code context. Murder, kidnapping and assault by terrorists are treated exactly the same as murder, kidnapping and assault by any other type of criminal. Other sovereign nations have chosen to create the offense of terrorism. They have legislated laws, which apply directly to the anti-terrorism effort. Some have been in place for quite a long time as in Northern Ireland and the Middle East. Others like those enacted in Canada to combat the FLQ have been short-lived. Like in all other criminal cases, the legislation is subject to review by the judiciary and is bound by the fundamental civil rights dictated. Other countries are not held by those same constraints.

Many nations have tried many remedies to control terrorist activity. New technologies become available with increasing speed to assist authorities in providing security at airports and onboard aircraft. However, all of these available technologies used by security personnel or anti-hijacking/rescue squads must be viewed in perspective and in the proper focus. Technology is not the bottom line. The human effort behind the security demands scrutiny as well. The current political sentiment has justified massive budget expenditures to militaries, police forces and other agencies. Such actions also have challenged constitutional personal rights to travel, to privacy and equal protection under the laws. It is clearly within every nation's best interests to harness the concern for airline safety. The key is to do so within acceptable democratic norms.

Each airline determines what procedures are appropriate for its own operation. In the recent past, however, the airlines have all come to realize that the threat is very real. Additionally, that very real threat has made it clear that security is cheap in comparison to the costs of a major security breach. The airlines have been forced to think the unthinkable. Namely that the cockpit is not secure, the terminal is not secure and the aircraft is not secure unless proper procedures and equipment are used to make them secure.

In accordance with the concept of awareness of the threat, the airlines need to take one step further and recognize that quick stopgap measures will prove to be insufficient. Furthermore, more of the unthinkable thoughts need to be addressed. Those unthinkable thoughts; including the threat of nuclear, biological or chemical attack will continue to plague the airlines and airports. New procedures and policies must be developed to meet these threats. The ebola virus released in one aircraft and transported thousands of miles across an ocean can potentially kill millions of people.

Reference Materials:

AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747

ACPA, 2001. Retrieved from: http://www.acpa.ca/newsroom.

Addis, Karen K., "Profiling for Terrorists," *Security Management*, Vol. 36, No. 5, May 1992.

AirDisaster.com, (nd). Special Report: Air India Flight 182; http://www.airdisaster.com/special/special-ai182.shtml.

"Advanced Solutions for Weapon Screening and Asset Protection," Ranger Security Detectors, El Paso, Texas, 2001.

Born, M. and Wolf, E., 1964, Principles of Optics, New York.

European Community Radiological and Nuclear Medicine Installations Regulation 1998- Regulation 8

Electronic Privacy Information Center, Transportation Agency's Plan to X-Ray Traveler's Should be Stripped of Funding. (June 2005). Retrieved from: http://www.epic.org/privacy/surveillance/spotlight/0606/.
Canadian Aviation Bureau Aviation Occurrence, Air India Boeing, 747-237B VT-EFO Report
Congressional Research Service ˜ The Library of Congress"

Convention on International Civil Aviation, Annex 17.
Defining Multi-Zone Detection: Check Apple for Apples. (3 May 2001). Retrieved from: http://www.omnisecurity.com/wthru2/wtindex.html. pg 2,3.

Federal aviation Regulations Part 121Guzzo.R.A. (1988). Productivity in

Organizations, San Francisco, CA: Jassey-Bass.

Hardage, M.L., Marbach, J. R., Winsor, D.W., “The Pacemaker Patient and Diagnostic Device Environment”, Modern Cardiac Pacing, Futura Publishing Company, Mount Kisco, NY, pg. 857-873, 1985.

How a Metal Detector Works. (24 July 2001) Retrieved from: http://micro.magnet.fsu.edu/electromag/java/dectector/. Pg 1.

Indian Kirpal Report, Report Of The Court Investigating Accident To Air India Boeing 747

Aircraft VT-ETO, “Kanishka” On 23rd June 1985

Ionizing Radiation Regulations 1999, UK, (Statutory Instrument No. 3232).……., “A Performance Evaluation of Biometric Identification Devices”, Sandia Corporation, UC-906, June 1991

National Research Council, “Airline Passenger Security Screening, New Technologies and Implementation Issues”, Publication NMAB-482-1, National Academy Press, Washington, D.C. 1996.

National Crime Prevention Institute. (1986). Understanding Crime Prevention, Stoneham, MA: Butterworth Publishers.

NAVAVNSAFECEN Investigation 69-67, RA-5C, 14 June, 1967
Naudts. John, (1987). Access Control: It’s in the Cards. Security Management, ASIS, pg. 169.

Morris, Jim. (19 Feb 2001). Since Pan Am 103, a Façade of Security. US. News, Retrieved from: http://www.usnews.com/usnews/issue/010219/safety.htm. pg 1-3.

Report of the Standing Committee on National Security and Defence. (January 2003). The Myth of security at Canad’as Airports. Second Session Thirty Seventh Parliament . Retrieved from: http://www.parl.gc.ca/37/2/parlbus/ commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.pdf.

Radiological Protection Act of 1991 Irish Legislation- Section 2
United Nations Scientific Committee on Effects of Atomic Radiation,

UNSCEAR, "Sources and Effects of Ionizing Radiation, United Nations, NY, 1994.

Bob Rae. (2005). Lessons to be Learned on Outstanding Questions with Respect to the Bombing of air India Flight 182, Ottawa: Air India Review Secretariat. Retrieved from: http://www.cbc.ca/news/background/airindia/pdf/rae-report.pdf

Rochelle, Carl.(2000). FAA Calls for Security Improvements at US Airports. Retrieved from: http://www.cnn.ru/2000/travelnews/01/07/bombandbaggage.

STUDIES IN DEFENCE AND FOREIGN POLICY, NUMBER 2 The Fraser Institute
10 Canadian Civil Aviation Security

Sweet, Kathleen M., *Terrorism and Airport Security*, Edwin Mellen Press, Lewiston, NY, 2002.

Sweet, Kathleen M., *Aviation and Airport Security*, Prentice Hall Publishers, Upper Saddle River, NJ.

TSA News Release. Retrieved from: http://www.tsa.gov/publuc/display?theme=44&content=09000519800cf9c8.

Wallis, Rodney. (2000). Lockerbie the Story and the Lessons. Praeger Publishers.

Additional Resources

The recent review by an Independent Advisory Panel of the *Canadian Air Transport Security Authority (CATSA) Act* and the corresponding body it established to implement and manage screening functions at Canada's airports.http://www.tc.gc.ca/tcss/CATSA/FinalReport-Rapport_final/final_report_e.pdf
The recent *Special Examination Report* of CATSA by the Auditor General of Canada: http://www.catsaacsta.gc.ca/english/about_propos/rep_rap/oag_bvg/CATSA%20Spec_Exam_E.pdf

A link to the Fifth Estate's investigative documentary, "Fasten Your Seatbelts", on aviation security in Canada: http://www.cbc.ca/fifth/fastenseatbelts/

Biography

I am currently an Associate Professor at the Virginia Commonwealth University and an Adjunct Professor at Embry Riddle aeronautical University and Goodwin College. I formerly taught courses in Aviation Security, Terrorism and Strategic Intelligence in the Department of Aviation Technology at Purdue University. I am CEO and President of Risk Management Security Group and am certified by the UK and Irish Department of Transport to teach air cargo security. I received my undergraduate degree from Franklin and Marshall College in Lancaster, Pennsylvania, in Russian Area Studies and a Master's Degree in history from Temple University. I have been admitted to the bar in Pennsylvania and Texas after graduating from Beasley School of Law in Philadelphia, PA. I am a graduate of many Air Force and civilian training programs.

After graduating from law school, I joined Wyeth International Pharmaceuticals as a legal specialist focused on licensing agreements between Wyeth and international agencies. I later joined the US Air Force and initially was a member of the Judge Advocate General's Department. I frequently served as Director of Military Justice at the base and Numbered Air Force level. After fifteen years as a JAG, and generally engaged in prosecuting cases on behalf of the military, I transferred to the 353rd Special Operations Wing as a military political affairs officer. I was later an intelligence officer assigned to HQ AMC as an executive officer and briefer. In 1995, I became an Assistant Air Attaché to the Russian Federation. As an attaché, I was engaged in liaison work not only with the Russian Air Force but also the Federal Security Bureau, at which time I became interested in counter terrorism efforts.

My final assignment was as an instructor at the Air War College where I taught in the International Security Studies division. I later became an Associate Professor at St. Cloud State University in the Department of Criminal Justice and an Associate Professor at Embry Riddle Aeronautical University; teaching security and intelligence related courses. I am the author of four books, Terrorism and Airport Security, (Edwin Mellen Preses, March 2002); Aviation and Airport Security: Terrorism and Safety (Prentice Hall Publishers, Nov 2003) and The Transportation Security Directory (Grey House Publishing, Jan 2005.) My fourth book, Transportation and Cargo Security: Threats and Solutions was published in late 2005.

My company, Risk Management Security Group, doing business in Ireland as RMSG Ireland Ltd., engages in all aspects of consulting in transportation-related security: including the preparation of threat and vulnerability assessments and security awareness training.