WORLD-CHECK™
REDUCING RISK THROUGH INTELLIGENCE

AUGUST 2009

Expert Talk

Hotel Security After Jakarta: Rethinking Faulty Assumptions

by John Solomon, Head of Terrorism Research, World-Check

Newsletter by World-Check, the recognised authority on reducing risk through intelligence.
www.world-check.com/experttalk

In response to hardened security measures after 9/11 in airports and embassies, terrorists have adapted by intensifying their focus on soft targets; namely, the hospitality industry. There have been myriad plots and at least 11 successful attacks on hotels from New York City to Mumbai since 9/11. Not only are hotels relatively easier to hit, they are also attractive targets due to their iconic landmark status. In addition, western businessmen and diplomats tend to meet and work there. While preventive measures are inherently limited – terrorists know when and where they will strike, counterterrorism specialists do not – there are still obvious gaps that need to be addressed to make hotels safer.

On July 17th, two suicide operatives executed a coordinated attack on the Ritz Carlton and JW Marriott hotels in an upscale area of Jakarta, Indonesia. Nine people were killed and over 52 injured. According to investigators, the operatives checked into the hotels as guests, hiding the explosives in their luggage and circumventing the physical security screen by using the trolley, which was too big to roll through the screener. The operative assumption held by the staff was that a hotel guest could not be a terrorist; thus leading the bellboy to decide that the luggage could be whisked away to the guest's room without any added scrutiny.

The aftermath of the Ritz Carlton and JW Marriott hotel bombings

There are two obvious problems with most hotel security programs that need to be rethought. The first is that hotel security measures are not adequately screening their guests and employees for possible terrorism risk. Terrorists must reconnoiter and access targets in order to increase the chances of a successful attack. Intelligence and access are requirements for a successful terrorist attack. When the target type is a hotel, the operative is likely to try to gain access to the hotel as a guest or employee. This tactic was used in almost every hotel attack. The attack cell in Jakarta had checked into the JW Marriot and Ritz Carlton as guests. The same is believed to be true of the Lashkar-e-Tayyiba support cell in place in Mumbai with respect to the Taj and Oberoi hotel siege in November 2008. An unconfirmed report indicated that one of the casing cells interned for 10 months as a chef at the Taj. This would explain why the terrorists in Mumbai had much greater knowledge of the hotels and security process than the commandos charged with securing them. In addition, an al-Qaida terrorist responsible for the September 2008 strike on the Marriot in Islamabad, a property described as a "fortress," also reconnoitered the property by checking in as a guest.

Even with every state of the art piece of physical security kit, a security approach is vulnerable if it lacks a process to identify, profile and screen the potential terrorism risk of those people entering the property. The security programs in place in hotels generally fail to assume that there is a real risk of a hotel guest being a terrorist. That leads to a major security gap that terrorists have exploited repeatedly. Staff from the cleaners up to the CEO should be aware of the type of terrorist threat the hotel faces and what red flags to watch for. It is understandable that hotels would not want to treat their guests as potential security risks or, even worse, terrorists; yet, client screening is far more discreet and much less obtrusive than invasive physical searches. The aviation and banking sectors have learned how to "know thy customer" in a way that is consistent with good customer service protocol while, at the same time, serves its critical function for terrorism prevention. Without intelligence on who is in the property, any risk management system has already greatly increased odds of failing.

"Staff from the cleaners up to the CEO should be aware of the type of terrorist threat the hotel faces and what red flags to watch for."

The second problem is that faulty analysis is informing the risk perceptions of the security and risk managers responsible for the hotel. A common practice is for security specialists to regularly provide threat assessments to the hotels to help them decide what precautions and measures should be taken at any given time. The problem though is that many security and counterterrorism specialists base threat assessments almost exclusively on the historical incidence of attacks. In essence, they assess that the future will be like the present and recent past, only more so. So if there has not been an attack in some years, they conclude the risk has significantly decreased. They largely ignore the festering growth and proliferation of a terrorist group and its capacities as key indicators of terrorism risk. Terrorist attacks do not happen in a vacuum. An effective terrorist organization requires infrastructure to facilitate militant training, ideological work, and propaganda to recruit more members. These things, in turn, cost money. JI – and I am referring to JI as short form for the al-Qaida-linked, Indonesian-based salafi jihadist network -- has appeared active for the past 4 years building and growing the organization. Yet many in the security field averred in the months and weeks leading up to the latest attack in Jakarta that the JI threat had somehow dissipated. The same argument was advanced regarding Lashkar-e-Tayyiba – its huge fundraising and recruitment activities since 2005 did not set off alarm bells until after it assaulted the Taj hotel last November. This analytical error stems from focusing on historical case studies of attacks rather than broad organizational capabilities and intent. It is a little like standing in the middle of the Pacific Ring of Fire, where the seismic interactions cause around 90% of the world's earthquakes, and thinking that the likelihood of an earthquake or volcanic eruption on a given day was low because there hadn't been any quakes in a few years.

The problem of ensuring security in luxury hotels is not an easy one. Service makes or breaks a hotel in the many starred end of the market. So hotels understandably do not want to trouble guests with complicated security procedures. Thus lowering the vulnerability of hotels to attacks like the latest in Jakarta will require more than merely increasing the number of metal detectors and guards. It will require intelligence-led solutions like customer and employee screening. This can be augmented by relying less on simplistic, linear analysis of current terrorist threats. Security managers should rely more on thorough evaluations of the extent and spread of a given threat group at any given time, judged by the concomitant threat it poses geographically in light of its precursor activities.

A holistic change in mindset must occur to reflect the real risk of a low probability but high impact event like a terrorist attack taking place. A 360 degree situational awareness must be had to manage possible security threats. It is to be seen whether those in the security community will learn from these clear lessons of the past. The terrorists, if history is any guide, most certainly will.