

## Security & Safety

### “Please Do Not Disturb”: Request for Privacy or Early-Warning Sign?

By Bruce McIndoe, President, iJet Intelligent Risk Systems



Mr. McIndoe

Co-authored by Efi Patt, Global Hospitality Practice Leader, iJET, a 3i-MIND Company

On the morning of July 17, 2009, a bomb was detonated in the lobby lounge of the JW Marriott Hotel in Jakarta, Indonesia. Approximately ten minutes later, a second bomb exploded in the Airlangga restaurant of the adjacent Ritz Carlton Hotel. The attacks, which killed nine and injured more than 50, were carried out by two suicide bombers identified as members of Jemaah Islamiyah, an Islamic militant group operating in Southeast Asia. This was the second attack on the JW Marriott Hotel in the last eight years. In 2003, a car bomb exploded at the hotel's entrance, killing 12 and injuring another 150.

Today, only bits and pieces of information are available to provide insight into the movements of the Jakarta bombers and their interactions with hotel staff in the days and hours leading up to the 2009 attacks. According to news reports, the JW Marriott bomber checked in to the hotel as a first-time guest two days before the attack, paid \$1,400 US in cash, was very particular about the room he was willing to accept and, despite being asked to do so by the hotel's reception staff, did not present his identification card upon check-in (granted, the photocopier was broken and the guest was asked to return at a later time). Apparently, the bomber spent the following two days in his guest room, assembling the bombs using components from the room's flat screen TV and hiding materials in an air handling unit located in the room's bathroom. Throughout this time, a “do not disturb” sign was displayed outside his room.

In the case of the Ritz Carlton Hotel, the bomber entered the staff entrance, supposedly to deliver flowers. It is thought that he may have passed through a tunnel that connected the Ritz Carlton and JW Marriott hotels and visited the JW Marriott bomber before returning to the Airlangga restaurant where he detonated the bomb he was carrying in luggage.

Taken together, the attacks represent a tactical shift by Islamic terrorists whose activities target hotels and similar “soft targets”. Previously, soft-target attacks were more likely to have been directed at hotels with little or no security, wherein perpetrators forcefully gained access to protected venues and immediately detonated ready-made explosive devices. But in the case of the 2009 Jakarta attacks, the terrorists unassumingly entered well-protected hotels as might a typical guest or vendor. They underwent security screenings and still managed to smuggle bomb-making materials into the hotel(s), where they later assembled their explosive devices.

Taken together, the attacks represent a tactical shift by Islamic terrorists whose activities target hotels and similar “soft targets”. Previously, soft-target attacks were more likely to have been directed at hotels with little or no security, wherein perpetrators forcefully gained access to protected venues and immediately detonated ready-made explosive devices. But in the case of the 2009 Jakarta attacks, the terrorists unassumingly entered well-protected hotels as might a typical guest or vendor. They underwent security screenings and still managed to smuggle bomb-making materials into the hotel(s), where they later assembled their explosive devices.

#### Awareness Training for Non-Security Staff

Hotel security typically offers limited coverage of hotel premises, covering only access points and public areas, such as guest and staff entrances, lobbies, parking garages, loading docks and hallways. Furthermore, security staff, cameras and other electronic surveillance measures are rarely present in conference rooms, hotel guest rooms, restrooms, and inside stores and storage areas. And finally, security personnel have limited interaction with guests and vendors and the limited number of security staff typically employed in hotels offer few opportunities to observe guests, visitors and vendors within the premises.

The attacks on the Jakarta hotels emphasize the need for hotel staff, including those not assigned to security tasks, to play an active and involved role in protecting hotel assets and facilities, guests and staff. Hotel employees regularly interact with guests, vendors, visitors and their own colleagues and are well-positioned to notice suspicious activity while carrying out their normal duties.

Hotel staff can be trained to mindfully look for, identify and report suspicious activity, delivering first-hand, early-warning intelligence to hotel management and security staff who can then take action to prevent or mitigate terror attacks and other criminal activity.

Awareness training should aim to accomplish the following:

- Map typical guest, visitor and vendor profiles for a given hotel so that employees can easily identify irregularities and/or unusual behaviors.
- Use examples to train staff to recognize what constitutes suspicious activity worth reporting and know how to report it.
- Ensure that staff experiences that give rise to security alerts and lessons learned are communicated and shared among all employees.

During training, emphasis should be placed on identifying early-warning signs, such as attempts to conduct surveillance and gather information about the hotel, or signs of stress or unusual behavior among guests, vendors and others—even co-workers. Ideally, staff members are incentivized to remain vigilant and engaged as well as comply with reporting procedures; they should be recognized or rewarded for their involvement.

Training should be conducted and repeated on a regular basis and include all members of staff, whether in-house or outsourced. Furthermore, training should be customized for each department or work area so that employees are made aware of suspicious signs in their respective areas; and corresponding procedures should require employees to inspect their work environments and note and report noteworthy incidents. See Table 1 for examples.

**Table 1: Awareness Training for Non-Security Hotel Staff**

<b>Non-Security Staff (by department)</b>	<b>Security Detail</b>
Reception staff	Note and report walk-in guests, guests paying cash, first-time guests who are particular about their room location and guests unable to produce proper identification.
Bell staff, waiters, other staff working in public areas	Note and report guests taking photos of the hotel structure, elevators and emergency exits; report suspicious packages and left luggage.
Purchasing and stewarding staff (deliveries & loading dock)	Be on alert for vendors who do not report to them soon after being announced by security.
Engineering staff	Conduct background checks on vendors; note and report any signs of tampering with hotel machinery or missing equipment and items, specifically chemicals, fuel and other substances or items that can be used to create an explosive device.
Housekeeping	Note and report suspicious guest behavior or equipment left in guest rooms, such as weapons, dangerous substances or bomb-making materials; report cases in which guests prevent room access over a number of days.
All staff from across all departments	Note and report guests entering back-of-house areas, visitors roaming on guest-room floors, guests without a key asking to be let into rooms and vendors working outside their assigned areas; receive and accompany vendors to their work locations and monitor their whereabouts.

Special attention should be given to train housekeeping and in-room dining staff who work in guest rooms and on guest room floors—areas rarely covered by security. Housekeeping can alert security staff if access to a guest room is prevented (e.g., if the “do not disturb” sign remains hanging on a door’s exterior over the course of several days), indicating that there may be a problem concerning a guest. With proper training and high awareness, housekeeping staff will know how to identify and report suspicious items left in guest rooms, such as weapons, dangerous substances or explosives and bomb-making materials.

**Clear Processes and Procedures are Essential**

Clear reporting procedures and tools to manage and analyze indicative information are essential to ensure that early-warning signs are not ignored and that pieces of information gathered from multiple sources are combined to form actionable intelligence on suspected persons and suspicious activity. While reports of irregularities may not always amount to early-warning signs, put together, they may have intelligence value that can help security managers take preventative action to foil attacks or prevent criminal acts on the premises.

**Added Benefits of Non-Security “Security” Personnel**

The presence of security personnel is often perceived by hotel management as a hindrance to creating a hospitable and welcoming environment for hotel guests. Hotel guests have an expectation of privacy, which they may feel is violated by a large, visible security presence. Security personnel, who are often contracted staff, can have difficulty blending in and guests may frown upon having to undergo security checks. Blending security with guest services may help reduce this notion and involving non-security staff in a hotel’s security program may help increase overall security presence while reducing both the number of security personnel required and related costs.

*Bruce McIndoe is President of iJET, a 3i-MIND Company. An iJET founder, Bruce has been the key contributor to the company’s strategic growth, securing its position as a leader in business resiliency with the development of the Worldcue® Global Control Center. Under Mr. McIndoe’s leadership, iJET has grown from a start-up to an established global provider of travel risk management services for more than 500 organizations in the public and private sectors. With many years of experience in intelligence operations and information technology, Mr. McIndoe is a seasoned expert in travel security, intelligence and risk management. He has more than 30 years of experience in the planning, design, development and deployment of a number of large, world-wide intelligence and risk-management systems. He is also involved in the integration of Internet technology and application integration frameworks to support group work throughout the enterprise. Mr. McIndoe can be contacted at 410-573-3860 or [bruce@ijet.com](mailto:bruce@ijet.com)*



The Hotel Business Review is a weekly journal of best practices in hotel management and operations and is available at [www.hotelexecutive.com](http://www.hotelexecutive.com). HotelExecutive.com retains the copyright to the articles published in the Hotel Business Review.

Articles cannot be republished without prior written consent by HotelExecutive.com.