HOSPITALITY ATTACKS:
TIPS FOR GUEST SAFETY AND PROTECTION

Preparing a hospitality property for a hostile attack, including a review of security assessments, staff training, response plans and active shooter response.

BY ELIZA SELIG AND FRANK WOLFE, CAE

Pineapple Search℠
Produced by HFTP

HFTP®
Hospitality Financial and Technology Professionals

TABLE OF CONTENTS

AUTHORS

Eliza Selig is the director of communication for Hospitality Financial and Technology Professionals (HFTP®). She has been with HFTP since 1999, overseeing the association's communications endeavors, including serving as editor of the association's journal *The Bottomline*.

eliza.selig@hftp.org

Frank Wolfe, CAE is the CEO for Hospitality Financial and Technology Professionals (HFTP). He has been with HFTP since 1991, where he oversees the association's operations, as well as represents the association worldwide at industry events, on industry boards and committees, and via the news media.

frank.wolfe@hftp.org

Hospitality Financial and Technology Professionals
Global Headquarters
11709 Boulder Ln, Ste 110
Austin, Texas 78726
+1 (512) 249-5333 • (800) 646-4387 *(US only)*
www.hftp.org

FORWARD

Publishing something like *Hospitality Attacks: Tips That Could Save Lives* is just a bit outside Hospitality Financial and Technology Professionals' (HFTP®) regular educational offerings. HFTP is a global, nonprofit hospitality association that uniquely understands the industry's problems. It is recognized as a spokes group for the finance and technology segment of hospitality. We assist our members in finding solutions to industry problems more efficiently than any organization via our expert networks, research, conferences such as the Hospitality Industry Technology Exposition and Conference (HITEC®), and certification programs. HFTP has more than 5,000 members and several thousand stakeholders across the globe.

In order to fulfill our mission, HFTP has also developed the world's first industry vertical search engine: PineappleSearch.com, built by hospitality, for hospitality. It was named and designed so that an hospitality industry professional could quickly access relevant information, without having to wade through search result clutter. It was through that endeavor that this feature came to be.

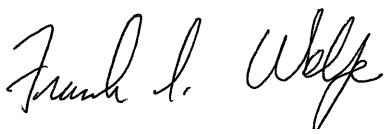
The Bataclan Theatre

During a business trip in Paris on December 16, 2015, about one month after the November 13 terrorist attacks on that city, I had the opportunity to pay respects to the many people who lost their lives on that unfortunate day. I visited The Bataclan theatre, one of the attack sites where an impromptu memorial had erected. It was a very moving and surreal experience, where colorful tributes of flowers, notes, drawings and photos were left in honor of those who perished in the attack. I snapped several photos of the site (above, right) and have altered one to resemble a painting, shown in the header above.

As it happened, the next day in Maastricht, I met with our partners at Hsyndicate.com to discuss marketing strategies for Pineapplesearch. One of the items on our agenda was to get people to subscribe to Pineapplesearch to take advantage of its customizable features. With The Bataclan memorial fresh in mind, I started searching for written information to see what was available for the industry on these kinds of events and found very little. Even after using Pineapplesearch for a deeper dive, it became apparent that there were few major articles on attacks on hospitality properties, and there was definitely room for a good one. I knew this would be a big undertaking, but it would be an important resource that HFTP could develop.

I contacted Eliza Selig, HFTP director of communications, to see if she would put her talents to the project; to which she agreed. Since we started working on this project, other events have occurred and our intentions are not to slight them in anyway. However, if you look closely at The Bataclan memorial, you will see things that hospitality is responsible for every day, all over the globe. These things are hope, memories, love, peace, honor, respect and even beauty.

HFTP hopes that this feature, *Hospitality Attacks: Tips That Could Save Lives*, becomes a valuable resource for the global hospitality industry.



INTRODUCTION

After the recent November 2015 terror attacks in Paris hit near busy, entertainment venues: outside restaurants, bars and the soccer stadium, there has been a rise in concern about the security at hospitality venues. The attacks garnered worldwide publicity and comment, part of the strategy behind the string of terrorist attacks happening across the globe.

In addition, within the past three months hotels have been targeted for terrorist attacks with armed assaults. On November 20, 2015 the Radisson Blu in Bamako, a luxury hotel in Mali was attacked by gunmen, killing 20. More recently on January 15, 2016 the Splendid Hotel in Burkina Faso had a hostage situation that lasted hours and ended with 29 people dead. An al Qaeda-linked terrorist group claimed responsibility for the assault. Additionally, as we were wrapping up this report, a Paris man with two firearms and ammunition in his luggage was stopped by security at the Hotel New York just outside of Disneyland Paris. He was stopped by a routine security checkpoint when his suitcase passed through an x-ray. While his intentions haven't been confirmed, this demonstrates the importance of security checks.

This list continues as we search through news archives from the past decade and more. Our aim is not to raise an alarm, but rather to demonstrate the reality that hotels are considered prime soft targets for attacks that seek to gain notoriety. With the possibility that you and your guests might face such a scenario, it is best to prepare you and your team to elicit the best outcome.

Why are hotels targeted? Hotels are considered soft targets that, when attacked, bring wide publicity. A soft target is "a person or thing that is relatively unprotected or vulnerable, especially to military or terrorist attack."[1] This event could be anything from a mentally ill guest to a domestic fight to an armed assault in a hostage situation.

A 2009 report[2] from Stratfor Global Intelligence wrote, "Hotels are the quintessential 'soft targets.' They have fixed locations and daily business activity that creates a perfect cover for preoperational surveillance. Extensive traffic — both human and vehicle — inside and outside the buildings still goes largely unregulated. This is especially true for larger hotels that incorporate bars, restaurants, clubs, shops, pools, gyms and other public facilities that cater to clientele besides the hotels' own guests."

A more recent assessment by the firm after the recent hotel attacks stated, "by attacking international hotels in capital cities that cater to Western business travelers, diplomats, intelligence officers and journalists, attackers can ensure that they gain significant international media attention without having to attack a tougher target such as a modern embassy."[3]

"Hotels are the quintessential 'soft targets.' They have fixed locations and daily business activity that creates a perfect cover for preoperational surveillance. Extensive traffic — both human and vehicle — inside and outside the buildings still goes largely unregulated."

–Stratfor Global Intelligence

So how does an industry that is required to offer a relaxed, discreet, unobtrusive and unencumbered experience for guests, reconcile those goals with offering guests a secure environment? Understanding that there is potential for danger, hospitality properties need to counter it with preemptive response planning. It is imperative for organizations to implement appropriate security measures, collaborate with local authorities and train staff in proper prevention and reaction methods. With the right planning a bad situation can be ameliorated.

GOVERNMENT RESPONSE

The wave of attacks has brought forward a series of responses from municipal, state/provincial and federal governments. This includes increased surveillance, having a more visible presence, and developing training and intelligence sharing programs for the public.

As seen over and over again, governments respond to such attacks by pledging greater security and surveillance. For example, in early January 2016, the Egyptian government stated they would invest US$32 million to upgrade security in two Red Sea resort areas popular with foreign tourists in the wake of a recent knife attack in front of the Bella Vista Hotel in the Egyptian resort town of Hurghada. The move is to restore confidence in the area's lucrative tourism industry. The funds will go towards security cameras, scanning and detection equipment as well as sniffer dogs. Broader than this example, France has stepped up its intelligence game in the wake of the two major 2015 terrorist attacks in Paris, as has countries the world over.

In addition to intelligence gathering, many police forces are getting specialty training in emergency response tactics. In past decades, when responding to an active threat, the method of operation had been to establish a perimeter and then wait until a SWAT team or hostage negotiator arrived. This tactic loses out on crucial time as the shooter continues his/her assault without confrontation. The goal now is to immediately neutralize the threat upon arrival.

The turning point in emergency response happened in April 1999 when two high school students in Columbine Colo. USA engaged in a shooting spree inside their school. In *How to Counter Armed Assaults* by Scott Stewart, vice president of tactical analysis for Stratfor, he explains, "In the aftermath of Columbine, officials learned that while the police established the perimeter and waited, the two attackers continued to kill students inside the school. Clearly while a shooter was actively killing people, the police could not just sit back and wait for specialty forces to respond to the scene. Moreover, since it often takes time for the specialized units to mobilize and respond, such a delay can prove deadly."[4]

The protocol for first-responders is to quickly form a team and neutralize the situation. To prepare, police departments are required to undergo additional response training and are given more powerful firepower such as shotguns.

Since then, the protocol for first-responders is to quickly form a team and neutralize the situation. To prepare, police departments are required to undergo additional response training and are given more powerful firepower such as shotguns.

This tactic is spreading globally. Stewart writes, "the Malian and French special operations forces actions during the Bamako attack and the Afghan government's response to several armed assaults in Kabul highlight that the concept is being spread to other governments through training programs such as the U.S. State Department's Anti-Terrorism Assistance Program and its Department of Defense equivalent, as well as through training provided by European and Australian forces."[4]

Governments are also working together with the public to help them prepare for an active shooter situation. The U.S. Department of Homeland Security has issued the directive: "Run, Hide, Fight." distributing guidance through a multi-media campaign (watch the video). Similarly, the United Kingdom promotes "Run.Hide.Tell." (watch the video).

In an interview with Stewart[5], he suggests that this information campaign has shown effectiveness by establishing response awareness, citing the attack in Bamako as an example. He explained that people

SECURITY TIP

The level of response training of government authorities varies by region and country. It is best to consider this when you are preparing and training for your property's emergency response, and investigate what is available in your area. The availability (or lack) of resources can determine how you develop your security plan.

in the hotel were able to avoid harm because they ran and took shelter behind locked doors.

On a municipal level, city governments work with the public on a back and forth dialogue for exchanging information. Many municipalities offer public awareness, response training and intelligence sharing programs. As an example, the New York City Police Department (NYPD) has NYPD Shield which, "provides training services to assist public and private sector entities in defending against terrorism."[6] As part of its educational arm, NYPD representatives lead informative programs such as a recent seminar it held for restaurateurs. The program instructed on best practices in responding to an active shooter within their facilities.

Paul Tormey, general manager of the Fairmont Copley Plaza, which is right on the route of the Boston Marathon, said that since the 2013 Boston Marathon bombing, there has been increased communication between the Boston Police Department and the public. He said, "We've gotten a little more diligent in our communications protocol, more than anything else. There is a heightened awareness in our communications process. Authorities send out e-mail on crime in the neighborhood and notify on events that may be happening so that we can stay more alert." [7]

The level of response training of government authorities varies by region and country. It is best to consider this when you are preparing and training for your property's emergency response, and investigate what is available in your area. The availability (or lack) of resources can determine how you develop your security plan.

INTERVIEW

ESTABLISHING HOTEL SECURITY

Hotel security expert Yitzhak Yerushalmi talks security best practices

He explains: A security plan that accurately incorporates procedures, personnel and technology can produce optimal security with a minimal budget

What are some of the factors you look for when doing a security assessment of a hotel to determine the type of security plan needed?

The parameters are numerous, but the most important ones are, first you must examine the security threats and risks in the geographical area (state, county or city) where the hotel is located, such that could have a negative effect on the hotel, be it direct or indirect. You must then analyze and define the extent of this risk: high, low, specific to the review period, permanent and so on.

Next, profile the guests. The more prestigious the hotel is, and the more it hosts dignitaries, celebrities, politicians, company owners and foreign nationals, the more likely it is to attract serious illegal activity, from terror attacks to espionage, information theft, kidnapping, attacks on dignitaries and more.

In addition, there are other restrictive parameters that must be taken into account during planning: an examination of the laws and regulations regarding businesses and hotels in particular in the country and city where the hotel is located. Also, what is the hospitality concept of the hotel management or owner? A hotel is built specifically to provide a lodging experience, and thus any security plan must be fully compatible with said concept. Any plan that doesn't fit in with the service given to the guest will be difficult to implement by employees and managers who aren't security personnel.

Yitzhak Yerushalmi has 30 years of experience in the field of security and defense, an expert in physical security consulting and training, managing complex projects which integrate modern technology, quality personnel and procedures. He's served as a security consultant for TAJ Hotels Resorts and Palaces, Tata companies, Inbal Jerusalem Hotel, Israel Hotel Association, Dan Hotels, Fattal Hotels, Club Hotels, Crowne Plaza Hotels and more.

What are the unique security issues to consider for a hotel vs. other public spaces?

A hotel should not be compared with any other public space. Yes, hotels also have public areas (lobby, restaurants, conference halls and spa) that legally anyone is allowed to enter and move around in, but that's the only parallel. There are many difficulties, but the greatest ones are: guests and other visitors. The hotel tries to provide a private lodging experience to guests who pay top dollar, much like luxury residential complexes that provide complementary services. But in contrast to them, it cannot prevent people from entering its perimeter, using some of its services and subsequently exposing its guests to many dangers that are difficult to monitor.

There is a strong tension between the desire to maintain effective security (as is customary in other places) and the desire to provide outstanding service and hotel experience. The franchise

executives and hotel managers tend to focus more on accommodation than on overall security, if at all. This creates quite a few opportunities for crime or acts of terror. Security personnel, especially those stationed at the hotel entrance, perform other tasks not necessarily related to security, such as carrying luggage, opening doors, answering guests' questions on various topics, parking cars, etc. This is a result of a shortage in manpower, the management's desire to save costs or vague job descriptions.

A hotel can host major international conferences, prestigious exhibitions, conference calls of countries and companies, and accommodates dignitaries — all in a small, unmonitored and uncontrolled area that is often not manned with armed guards, making it a soft and attractive target for terror attacks.

How do you balance a high level of security that might be needed vs. not being so confrontational in an environment where a sense of comfort is sought (i.e. a hotel)? Or is a security presence important in an area that is on high security alert?

It's possible to strike a balance in accordance with the requirements of both the state and the client if the security approach is changed. For example, at a luxury five-star hotel in Israel with 335 rooms that employs approximately 100 shift workers, the number of security personnel ranges from 4 to 5 percent, not including the head of security. In such a case, it is best to carry out visible security activity using various means (cameras, checkpoints, etc...) in high friction with guests and visitors in order to create deterrence and achieve effective security.

In contrast, if in the same hotel we distribute the security tasks among over 80 percent of the staff, while ensuring that they're trained and instructed as part of their position — we can increase collective awareness and vigilance and tighten the hotel's defense against the threats. In addition (and equally important), we will instill a desirable sense of security among the guests and also change the method of operation for dealing better with the real threats and risks.

What are some technologies that have been effective for security? What are some best practices?

Hotel security must include high quality personnel, good technology (which there is in abundance) and procedures. I've seen hotels with more than 400 cameras, checkpoints and x-ray scanners that failed to achieve a decent level of security precisely because of the hotel's dependence on technology. Nevertheless, it is worth it to invest in technology in sensitive spots in the hotel, such as guest rooms (intricate door locks, safes, door between rooms and so on), operational areas and outdoor areas, focusing on entrances to the hotel. A proper concept that accurately incorporates procedures, personnel and technology can produce optimal security with a minimal budget.

What are some basic security practices that you can train your employees with?

The focus at work must be on preventive security. If we take a terror attack for example, the hotel doesn't have the tools or the ability to handle such an event. It's possible to teach and train the hotel staff on how to deal with intelligence gatherers who come to choose their target. An early detection of these operatives or regular effective actions could prevent the planning of a terror attack or crime on hotel property. Both in terms of planning and execution, the hotel should provide a solution as far away as possible in the adjacent areas outside. Any potential solution must be proactive in the sense that it deters, not only alerts.

In your experience, what have been changes to the type of threats you protect against?

I think the following factors must be considered: recently more and more terror organizations see hotels as soft targets that promise high success rates, serious damage to the economy, that is — hurting inbound tourism, and a negative psychological impact on the sense of security in the country.

Due to the global economic situation, luxury hotels, particularly in third world countries, pose as attractive targets for crime organizations and sophisticated criminal gangs. There is an increase in credit card sting operations, information theft through Wi-Fi networks, theft in general (vehicles, embezzlement, fraud by employees), attempts to hurt public figures, or kidnapping. The comfort and services provided to every hotel guest also benefit those who want to commit a crime within the hotel's perimeter and its rooms. Hence, so long as the economic situation in the country/city in question continues to deteriorate, we will witness an increase in crime in hotels in general and luxury hotels in particular.

What are some best practices in case of an attack? What are your recommendations for responding once an attack has happened?

It's not possible to respond swiftly, but there should be a security separation between the open public areas and the floors housing the guest rooms. A proper mechanism that provides solutions for the public areas will allow keeping the damage to a minimum. ■

PREPARATION IN HOSPITALITY

There is no doubt that a security plan is necessary for any hospitality property. Even if the threat level in your area is low, as a high traffic public venue, the potential for a security emergency is likely. Your property most likely has a security plan in place already. If so, still consider the information below, because it could address situations that have not been considered.

Security Assessment

To get started, have a physical security assessment conducted for the particular property. This includes an evaluation of the area's crime levels and political stability, and whether your security system is sufficient to meet the potential threats for the region. Depending on the results of the assessment, management can determine what kind of resources need to be spent on for security and its support. If you are part of a larger hotel company, reach out to the corporate office to see what kind of assessment program is available to you.

An important consideration when going through with the study is to understand the level of training the local police force has in emergency response. The type of training local enforcement has, which varies by locale, determines what kind of private security you employ and the type of training you provide. As mentioned above, the tactic of a police force quickly neutralizing a situation is one that is being adapted worldwide, but not every police department necessarily has this level of training. It is good to plan for that scenario in case of an emergency. You don't want to depend on support that might not be there. If you do find that your local police force is trained to respond to an active shooter situation (or other hostile attack), it is valuable to know how they are trained to respond. If you and your team are familiar with their methods, you know what to expect and how best to assist them in neutralizing the situation.

In either situation, it is a good idea to establish a liaison with the police department so that you have a good line of communication with law enforcement. Your liaison will keep you apprised of potential threats in the area and the familiarity would likely help in the time of need. Also consider inviting the law enforcement team for a walkthrough of the property. This helps them get to know its layout and can navigate through the property that much more quickly in an emergency. You might go so far as to run practice drills with a SWAT team — although it might not be possible with the 24-hour nature of the business.

Security Equipment

Based on the area's threat level established by your security assessment, numerous physical and technological measures can be adopted. Some physical security measures include:

- ***Visible security*** – Place signs of security in obvious areas that can be seen to show that security is in place. This includes cameras and personnel.
- ***Landscape barriers*** – Build large barriers around the property to prevent vehicles from getting close to the building or driving in, which could deploy a bomb. This includes large planters, trees or other concrete barriers.
- ***Protective window film/bullet proof glass*** – Large windows are a common feature to hotel properties. While they are an important part of the ambiance, they can also be a danger. Line windows with a protective film that prevents them from shattering and reducing glass shrapnel in case of an explosion. Or depending on the threat level, consider replacing with bullet-proof glass.
- ***Automatic locks*** – Make sure that revolving doors and others to the exterior can be automatically locked to prevent the assailants from leaving quickly.

Investing in technology can also be a game changer. There are many monitoring products available that vary in cost. These systems use fingerprints,

facial recognition, radio frequency identification (RFID) and web interfaces to track movement throughout the enterprise and also to limit access.

Regardless of the size of your operation, accessible Internet Protocol (IP) cameras are inexpensive and easy to set up and monitor. Footage can be monitored from a smart phone and images can be pushed out to the Internet in real time, as well as store recorded images. If you are using cameras, make sure that the public is aware and you publish this fact.

The types of technology, enterprise investment, and (perceived) intrusiveness to your guests will vary depending on the type of hospitality enterprise, geographic location and many other factors. Some hotels in parts of the world have been using airport style scanners, sniffer dogs and private security for many years. Other parts of the world have virtually no security at all.

In December 2015, shortly after the Paris attacks, many major theme parks and retail establishments added airport style scanners, sniffer dogs, body searches, metal detectors, private security and armed police. Two weeks after, retail stores in the major shopping areas in Paris had long lines of customers waiting to get in due to wand searches implemented for guests' protection.

Prakash Shukla, is a managing partner with Solarex asset-management and was CIO at TAJ Group of Hotels, a Tata Group enterprise in 2008 when the property was held hostage by four gunmen. He attributes the CCTV throughout the large property as key to piecing together the events of the first hours of when the hotel was under siege.

Shukla said, "In fact we were able to put together an entire timeline of what happened, where the terrorists went in the hotel from the time the attacks started to the time at 5:00 a.m. or 6:00 a.m. the next day when the CCTV cameras were blown up because we lost power due to grenades. Until then, we had a good idea of the first 12 or 15 hours of what they did in the hotel and where they went. We were able to trace just through the network of CCTV cameras."[8]

Shukla recommends keeping the CCTV control room nearby or offsite so that the cameras can be accessed and controlled away from the property.

Staff Training

The biggest defense arm in your security plan is your staff. While you don't want to scare your staff with outlandish scenarios, they do need to be informed of the potential dangers that exist. Educate them on ways a criminal or terrorist could use your facility as a base for illegal activities, how they can help prevent an attack and what their responsibilities are in an emergency scenario.

One important step towards prevention is for all staff to know what constitutes suspicious behavior and be observant. Stewart said, "Many times people have a tendency to get over-confident of their security because of some of the electronic they have in place. Hey we have great CCTV. We have decent access control. They don't understand that those things are defeated a lot of the times. You can't become complacent because of the security measures that are there. You really need to have a lot of situational awareness, and the more situational awareness you have across the property, the better. There are just so many people in the hotel that have eyes on things that can see things before they develop, that the security staff may not pick up on."

In addition to an actual attack, there are numerous instances of criminal activity and planning that occurs within a hotel room. One of many examples of this was the December 1999 incident in which the "Millennium Bomber" Ahmed Ressam and an accomplice set up a crude bomb making production in a hotel room in Vancouver, B.C. Illegal activity and the

lead up to such activity can happen in all corners of the hotel, so it is crucial that all departments maintain awareness of guest activity,

Instruct staff to be the eyes and ears, and report suspicious activity to the security team. This includes when the person(s):

- Acts nervously and is overly concerned with privacy,
- Denies hotel staff access to a room, or refuses room cleaning during an extended stay,
- Insists on cash payment,
- Attempts to gain access to restricted areas or talks his/her way in to private areas, or
- Conducts surveillance of the property, including:
  - Takes notes, pictures or videos of the property
  - Sits in a car outside and watches the comings and goings of the property
  - Walks around the vicinity of the property, noting the different entrances
  - Circles security and observes security technologies (i.e. cameras).

Also have your staff note suspicious items, such as:

- Large amounts of unusual substances (acetone, peroxide, drain cleaner);
- Luggage emanating fumes or odors, or has disassembled electrical components (wires, circuit boards, batteries); or
- Plans, drawings, schematics, maps.

While the above behaviors do not automatically make the person(s) a criminal, such activities do merit further investigation, not a look the other way. If any of the above situations arise, instruct employees to promptly alert management and the appropriate authorities.

A big part of our business is hosting large groups for events. Such reservations come with advanced planning and an opportunity for you to take an extra security step and vet the organization or party. You can do this by researching the group; finding additional details as its history, purpose and recent activities. Also, during discussions with their representatives, you might consider having a conversation with them that covers more than event planning: asking if you've worked with them previously, or if additional security is needed and why. Finally, if the group has a public Facebook page for the event, ask if your property can be a member of the group. These simple steps can often alert you to potential issues.

MONITORING FOR SUSPICIOUS ACTIVITY

Instruct staff to be the eyes and ears, and report suspicious activity to the security team. This includes when the person(s):

- Acts nervously and is overly concerned with privacy,
- Denies hotel staff access to a room, or refuses room cleaning during an extended stay,
- Insists on cash payment,
- Attempts to gain access to restricted areas or talks his/her way in to private areas, or
- Conducts surveillance of the property, including:
  - Takes notes, pictures or videos of the hotel
  - Sits in a car outside and watches the comings and goings of the hotel
  - Walks around the vicinity of the hotel, noting the different entrances
  - Circles security and observes security technologies (i.e. cameras)

Response Plan

In addition to prevention, the worst case scenario must be planned for — develop a response plan. Response plans can be as unique as the enterprises that use them, but they should have information such as:

- A hierarchy chart that details staff responsibilities such as who is authorized to make decisions or serve as a communications liaison to press and via social media.
- Identification of the primary, secondary and tertiary evacuation points.
- First Aid Kits that include maps with all exits identified.
- Staff assignments to the various evacuation points, and documentation of these assignments. This also helps account for staff once the evacuation occurs.
- Noted staff members who have training in first aid or emergency medical training, or other useful skills such as second languages.
- List of employees and contact information.
- List of major vendors and the services they provide, along with the contact information.
- List of key clients and contact information.
- Property maps that indicate where the main switches are for utilities, the location of hazardous cleaning chemicals and other important site-related information. These need to be easily accessible to staff, outside security and first-responders. It is imperative that emergency responders can access floor plans away from the property to properly assess a response plan.
- Directions to the location of master keys and who can access these and under what circumstances.
- List of critical items that would be important to remove if possible.
- Sources for replenishing supplies if needed.
- A system in place that keeps a daily contract/corporate visitor list so they can be accounted for during an emergency.
- Resources to reference as guidance in the case of the emergency.
- Conduct practice drills and simulations with local law enforcement.

SECURITY TIP

All staff must be trained to react properly in the event of a crisis. Instruct them on the triggers that will set off the crisis plan and their responsibilities once it is in place. Each staff member should be assigned a role to help carry through the response in the best possible manner that is allowed.

- List of offsite computer, business intelligence and surveillance equipment.

With a crisis plan in place, it must not sit in a filing cabinet to get dusty waiting for the rare, but critical occurrence. Instead it should be reviewed, tested and updated on a regular basis. Managers need to know where it is located, as well as have it offsite and potentially on their mobile devices. To make sure this happens, assign a staff member(s) as the head of the crisis plan to follow-through.

As mentioned previously, your first line of defense and the most important is your staff. All staff must be trained to react properly in the event of a crisis. Instruct them on the triggers that will set off the crisis plan and their responsibilities once it is in place. Each staff member should be assigned a role to help carry through the response in the best possible manner that is allowed.

Not only should the team be aware of the plan, but drills should be conducted on a regular basis to practice the response. Discuss multiple scenarios — active shooter, hostage, bombing — and identify best exit routes and where to take cover. In the event of a real emergency, the response will most likely not go as planned, but having the framework will go a long way in helping set off an optimal reaction.

INTERVIEW

Social Media and Exceptional Staff Give Big Assist to Fairmont Copley Plaza Hotel During Crisis

The following is reprinted from HFTP's *The Bottomline* magazine, Summer 2013 issue, with a follow-up by Paul Tormey two years later.

By Frank Wolfe, CAE

The Fairmont Copley Plaza hotel is located just a city block from one of the bombs that exploded on April 21, 2013 as part of the terrorist attack on the Boston City Marathon and directly across the street from the marathon's medical tent. And because of its location the hotel became a major focus of concern for the hospitality community during that day's tragic event. Due to an exceptional staff, proper training and social media, the hotel's staff helped make many people safe, participated in the community responses and eased concerns from its community at large around the world.

I initially was caught up with the hotel's response to the bombings as I followed its notices on social media. From the messages, I knew the hotel's team had a lot on its plate and was acting with determined strength. As the weeks passed, I wanted to get in touch with the hotel management to get a better picture of how the events of that day unfolded and what kind of security plans were put into action. I had the opportunity to speak with **Paul Tormey**, the hotel's regional vice president and general manager. Unfortunately, Mr. Tormey is not a newbie to this type of situation. He is also responsible for hotels in New York City, and had to act after the attacks on the World Trade Center on September 11, 2001.

What advice would give to your colleagues to prepare for disasters in the future?
Hire the best people you can find. It always comes down to the people.

For decades, our hotel has been the headquarters hotel for the Boston Athletic Association, the organization behind the Boston Marathon. So in the days leading up to the race, we were in a soft lockdown due to our high profile guests. Plus, Fairmont Hotels has a significant training program that instructs staff on protecting guests and personnel in all sorts of situations.

With that said, it all comes down to your staff. Any time a tragedy like this happens, there is always a small amount of uncertainty about how staff will react when put under extreme stress like mine had to deal

with on that day. Any good general manager is going to try to prepare for anything that can go wrong, but the outcome depends on how the team reacts. In the hospitality industry, it's also how WE REACT.

Within a half hour of the bombings, your hotel was using social media and posted a statement on your Facebook page. How did technology assist you that day?
Accounting for our guests and staff safety was our primary concern. But, we did want to assure concerned people that we were safe as soon as possible. My e-mail inbox went from 13 to 350 e-mails within minutes. These messages were from all over the world. In order to respond quickly, we decided to post a statement on Facebook. This was a big help in getting the word out since there was a lot of misinformation about the hotel in the early hours of the tragedy. We have a protocol process in our hotels for crisis communications. This protocol was also very important to us since we needed to make sure that the message being conveyed was factual and timely as possible.

Our hotels have very good security protocols and those are always followed. Entrances and exits were monitored by security; staff, guests and VIPs were badged, and surveillance cameras were monitored and tapes handled appropriately. Although our cameras were not in view of the actual bomb sites, we did assist by turning all of our surveillance over to the FBI.

Follow-up Interview

I spoke with Paul on February 2, 2016 to see what kind of security measures had been implemented at the Fairmont since the 2013 Boston Marathon bombings.

What kind of impact on security did the bombings have?
Things changed a little bit. I would say the biggest adjustment we've made was the knowledge that something horrific like that could happen. It was no longer theoretical. We've gotten a little more diligent in our communications protocol, more than anything else. There is a heightened awareness in our communications process. Authorities send out e-mail on crime in the neighborhood and notify on events that may be happening so that we can stay more alert.

We have increased some of our locking systems for back of the house areas to make the hotel more difficult for someone to get in that shouldn't be here. Normal stuff, we just enhanced it. We recognized that when we did the lock down after the bombing: did we really lock it down or could someone get in, pretending to be a guest? We feel we've since secured the back of the house in a much better manner.

I think even more so than when the bombings occurred, we've prepared for active shooters. We've done some training in the last 30 days on that. Debriefed our security leadership, ran it by the executive committee here in the hotel, and have encouraged all departments to be familiar with the best means of access outside of the building. If you had to hide, where would you hide and how would you do it? And actually have had people physically practice their escape. So that's really not so much a result of the marathon bombings, but just a result of what continues to go on in the world.

How has the community moved forward?
The year after the bombings, the marathon was such a literally glorious, glorious day. The weather was beautiful, the temperature was right, the security was significant — to the point that it was a little overdone, but everyone kind of got it. The year after was the same thing. There was a sense of civic pride and the chip on the shoulder: "you can't hurt us." Now we continue with the idea of: never forget – keep vigilant, do what you need to do. You need to stay focused every day. If you see something, stay something. The basics.

We haven't made any huge changes, but maintain an awareness that something like that could happen and you've got to stay on your toes.

ACTIVE SHOOTERS

There have been multiple methods used for attacking public arenas, and in the past decade there has been a shift from bombs to armed assailants. If you were to find your property under attack by gunmen consider the directive distributed by the United States Department of Homeland Security RUN. HIDE. FIGHT.[9]

The steps in the suggested response are:

RUN. (If there is an active shooter in your vicinity)

- If there is an escape path, attempt to evacuate
- Evacuate regardless whether others agree to evacuate or not.
- Leave your belongings behind
- Help others if possible.
- Prevent others from entering the area.
- Call police when you are safe.

HIDE. (If evacuation is not possible)

- Lock and/or blockade the door. Move away from the door.
- Silence your cell phone and turn off vibrate mode.
- Hide behind large objects and if possible find reinforced walls.
- Don't trap or restrict your options for movement.

FIGHT. (As a last resort and only if your life is in danger)

- Attempt to incapacitate the shooter.
- Act with aggression.
- Improvise weapons.
- Don't hesitate once you have committed.

Once First Responders are on the scene:

- Try to remain calm and follow instructions.
- Keep your hands visible.
- Don't hug them or thank them as you may hamper their ability to stop the shooter.
- Avoid yelling, screaming or waving your arms around.

Before you make your move and determine what your step will be — run, hide or fight — you must first determine where the threat is coming from. The key is not to act blindly, but to know where the danger is. Fortunately, most active shooters are poor marksmen, so it is best to get as much distance as possible from the shooter.

Scott Stewart notes, "This typical lack of marksmanship implies that most people killed in active shooter situations are shot at close range. Thus, it behooves potential victims to move quickly to put as much distance between themselves and the threat. Even the act of moving, especially if moving away at an angle, makes one a much harder target for a poorly trained marksman to hit."[4]

Once you have distance, aim to get cover rather than conceal yourself for best protection. A cover would be something that would prevent you from being pierced by a shot or at least dissipate the impact of a bullet. Such cover could be a heavy piece of furniture or metal filing cabinet. Your next option would be to conceal yourself by hiding behind a barrier such as a locked room. Note that although you are concealed and out of site, like hidden behind a bush, you would not be protected by a bullet. The advantage to a hotel property is that there are many rooms where you can take shelter behind a locked door. If you are sheltering with a group of people, decide on a plan of action if discovered by the assailant(s).

CONCLUSION

Although incidents of the nature discussed here are often on the news, it is very unlikely that you or your guests will ever find yourself in a situation like this. To try to calculate those odds realistically, Michael Rothschild, a former business professor at the University of Wisconsin, worked out a couple of plausible scenarios. For example, he figured that if terrorists were to entirely destroy one of America's 40,000 shopping malls per week, your chances of being there at the wrong time would be about one in one million or more. Rothschild also estimated that if terrorists hijacked and crashed one of America's 18,000 commercial flights per week that your chance of being on the crashed plane would be one in 135,000. In other words, your risk of dying, or being involved in one of these events is much lower than your risk of dying in a car accident, by walking across the street, by drowning, in a fire, by falling, or by being murdered. With that said, when you are overseeing a very public location such as a hospitality property, make the move from soft target to hard target. In the rare case you are involved in such an attack, your response will make a key difference on the level of impact it has.

Disclaimer: The information contained within this article if for general informational purposes only. Neither Hospitality Financial and Technology Professionals (HFTP), nor any of its staff, affiliates or partners, shall be held liable for any improper or incorrect use of the information described/and or contained and assumes no responsibility for anyone's use of this information.

Sources:

1. Soft target, Oxford Dictionaries Online.
2. September 8, 2009. Stratfor Global Intelligence. Special Security Report: The Militant Threat to Hotels.
3. Stewart, Scott. January 21, 2016. Stratfor Global Intelligence. *Lessons in Protective Intelligence*.
4. Stewart, Scott. December 3, 2015. Stratfor Global Intelligence. *How to Counter Armed Assaults*.
5. Interview with Scott Stewart, president of tactical analysis for Stratfor Global Intelligence, conducted on January 26, 2016.
6. NYPD Shield. http://www.nypdshield.org/public/
7. Interview with Paul Tormey, general manager of the Fairmont Boston, conducted on February 2, 2016.
8. Interview with Prakash Shukla, managing partner with Solarex asset-management, conducted on January 25, 2016.
9. Department of Homeland Security. *Active Shooter Pocket Card. https://www.dhs.gov/sites/default/files/publications/active_shooter_pocket_card_508.pdf*

ABOUT HFTP

HFTP, founded in 1952 and headquartered in Austin, Texas, USA with additional offices in Maastricht, The Netherlands, and Kowloon, Hong Kong, is the global professional association for financial and technology personnel working in hotels, clubs and other hospitality-related businesses. HFTP provides first class educational opportunities, research, and publications to members around the globe including, the premiere hospitality technology conference HITEC — founded in 1972. HFTP also awards the only hospitality specific certifications for accounting and technology — the Certified Hospitality Accountant Executive (CHAE) and the Certified Hospitality Technology Professional (CHTP) designations.

MY HFTP

THE **HFTP** Network

MEMBERSHIP GIVES YOU ACCESS TO OVER **5,100** INDUSTRY PROFESSIONALS ACROSS THE GLOBE.

WORKING AT Hotels, Clubs, Resorts, Casinos, Suppliers and more

WITH TITLES SUCH AS CIO, Controller, Consultant, Professor, CFO, Systems Mgr, Director of IT, Accountant, General Mgr, Account Mgr

My HFTP **member benefits**

❍ Gain Know-how
Build a base of knowledge at one of HFTP's educational conferences, which members attend at a discounted rate.

❍ Tune In
Participate in free webinars for members on important industry topics each month and earn CEU credit.

❍ Communicate with Your Network
Interact with members with similar workplace issues as you through chapter and global events, and through the members-only, digital Community @ HFTP.

❍ Read Up
Review HFTP's publications: a quarterly digital magazine with industry best practices, *The Infoline* e-newsletter and the *HFTP Connect* blog.

❍ Keep Informed
Access the HFTP Research Institutes, with locations in the U.S. and Hong Kong, for current data on industry trends and practices.

❍ Get Certified
HFTP members get exclusive resources for the Certified Hospitality Technology Professional (CHTP) and the Certified Hospitality Accountant Executive (CHAE) designations.

MY HFTP — Your Hospitality Network

Join Today at www.hftp.org