Mitigating Rising Risks for High-Rises

By Joshua Sinai

1 March 2021

Print Issue: March/April 2021

Over the past 60 years, tall buildings were increasingly subjected to violent attacks—from shootings to car bombs to hijacked airplane crashes. In response, security departments in tall buildings have adapted to institute various access control-related safety protocols, technologies, and systems to minimize attackers' potential access to employees, contractors, visitors, and facilities.

To understand the magnitude and likely evolution of these types of violent threats against high-rise buildings, security professionals must assess the structural distinctions between tall buildings, the different types of attacks conducted against them over the years, the varying motivations that drive assailants to launch such attacks, and the countermeasures in place following these different types of vertical attacks.

Tall Building Types

In general, tall buildings can be grouped into **three categories**: high-rises, skyscrapers, and high-tower buildings. The threshold for a high-rise building is defined as higher than 75 feet—or about seven floors—and up to 328 feet. High-rises are tall enough that occupants would need to use an elevator to reach a top floor, and the top of the building is out of reach for firefighting equipment. The **term is subjective**, however; a 15-story building may be considered tall in a suburban environment, but the same building would be dwarfed by buildings rising 50 stories high in metropolitan areas. Additionally, environment matters for security—first responders in these areas would have different experiences with addressing threats in tall buildings, and risks are likely different for a notable 15-story building in a small town versus a 15-story building surrounded by skyscrapers.

Skyscrapers are at least 40 floors, or higher than 328 feet. Most skyscrapers are designed for office, commercial, and/or residential uses. A few notable examples include the Empire State and Woolworth buildings in New York City, New York; the Willis Tower in Chicago, Illinois; and the Shanghai Tower in Shanghai, China.

The final distinction is for buildings with high towers. While these edifices might not be skyscrapers, the upper portions are much narrower than the base of the building. Consider belltowers, steeples, rotundas, or tall pavilions on top of buildings. These towers may not contain large populations in and of themselves, but they can create a dangerous perch for a sniper or attacker to take aim at people below.

For instance, in August of 1966, Charles Whitman, a student at the University of Texas at Austin, opened fire from the Library Tower's observation deck, roughly 307 feet up from the ground. He maintained his position for one hour and 36 minutes, during which he killed 14 people and injured 31 others, not including his mother and wife, both of whom he killed prior to the shooting. His attack at the campus ended when he was shot and killed by Austin police officers.

Motivated and Methodical

For various reasons, violent actors select hard targets to either directly attack or use as a launchpad for attacks against other targets. Tall building attacks also carry a reputational element for attackers,

who may believe that evading and bypassing security to carry out a mass casualty attack solidifies their stature as destroyers.

From a tactical perspective, attacks from within tall buildings can be prolonged when response from security and police is delayed, especially to higher floors, hindered by the restrictive nature of the buildings' access channels, such as stairwells and elevators. Response can also be hampered by attackers' ability to move between floors.

Certain events are also notable for the turning point they represent for tall building security. In some instances, the presence of several armed terrorist operatives throughout a facility can vastly complicate law enforcement's ability to quickly overcome and apprehend the attackers. This was the case in November 2008 in Mumbai, India, when 10 terrorist operatives of the Pakistani Lashkar-e-Tayyiba group carried out simultaneous attacks on multiple hotels, including the Taj Mahal Palace and Tower Hotel, which resulted in a four-day siege and the deaths of at least 31 people. This siege was the first time a swarming attack on this scale had been used in an urban setting; Western counterterrorism agencies have since planned ways to address a similar situation against major buildings within their respective borders.

ATTACKS FROM WITHIN TALL BUILDINGS CAN BE PROLONGED WHEN RESPONSE FROM SECURITY AND POLICE IS DELAYED, ESPECIALLY TO HIGHER FLOORS.

Similar incidents of emergency or police responders hindered by either architectural design or attackers' efforts had happened prior to the Taj attack, leading to significant changes in operational and security responses. In October 2017, Stephen Paddock killed more than 50 concertgoers at the Route 91 Harvest Music Festival from his 32nd floor hotel room in the Mandalay Bay Resort and Casino in Las Vegas, Nevada. He created a sniper's nest from a position high above potential victims, stockpiling a large cache of weapons and ammunition in his hotel room, and using the hotel's "Do Not Disturb" policies to evade detection.

In response to the attack, several hotels began implementing short-term measures such as using handheld wands to scan guests' bags, increasing the presence of security officers, training staff to recognize suspicious behaviors, and being on the lookout for a guest who might leave a "Do Not Disturb" sign on his or her door for more than 24 hours.

Eight years after al Qaeda's 1993 attack on the World Trade Center, where a vehicle-borne improvised explosive device (VBIED) failed to bring down the two towers, the terrorist group returned to the site to try again. On 11 September 2001, the group's willingness to adapt and innovate its tactics was successful, with hijacked airliners proving effective weapons. How tall buildings are designed to accommodate evacuations—previously based on evacuating one floor at a time—was overhauled after the difficulty of emptying the towers prior to their collapse.

INCIDENTS INVOLVING ACTIVE SHOOTERS IN A HIGH-RISE—WHERE FIRST RESPONDERS' ACCESS TO TOP FLOORS CAN HINDERED BY THE CONSTRAINTS OF ELEVATORS AND STAIRS—HAVE INITIATED UPDATES TO SECURITY POLICIES AND MEASURES.

In July 1993, **Gian Luigi Ferri** walked into a high-rise building in San Francisco, California. When he reached the offices of the law firm Pettit & Martin on the 34th floor, he opened fire on the people there, roaming the floor. Afterwards, he used the building's internal staircase to move to floors below, killing eight people before committing suicide as police responded to the shooting. The incident was notable due to the fact that it took police only a matter of minutes to respond, aided by a call to emergency services moments after the first shot was fired.

Incidents involving active shooters in a high-rise—where first responders' access to top floors can be hindered by the constraints of elevators and stairs—have initiated updates to security policies and measures, such as installing security stations at entrances, use of employee identification badges allowing for specific access to the appropriate offices, and surveillance of vendors and visitors.

In certain U.S. states, tall buildings are required to implement emergency action plans (EAPs) and integrate all tenant employers under the command of the building's EAP director. These emergency plans also include response protocol guidelines, providing information on how to shelter-in-place, follow a partial or full evacuation, and use elevators or stairways during a crisis, because not all floors might be affected by an incident.

Other attacks have exposed security gaps closer to the ground. For example, the 1993 attack on the World Trade Center and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City were both perpetrated using VBIEDs. After these events, exterior defensive measures were enhanced to mitigate against the possibility of using car or truck bombs against tall buildings. These developments included installing bollards, concrete barriers, and even tiered landscaping to make it more difficult for attackers to station a VBIED near such buildings.

Another incident occurred on 25 December 2020, when a suicide bomber detonated a VBIED in Nashville, Tennessee. The explosion occurred in the city's downtown area, a welcoming neighborhood that typically attracts pedestrians to bars, restaurants, and businesses along its streets, many of which are narrow or one-way, including the particular block where the attack occurred.

Besides damaging several buildings, the explosion also injured eight people. Given that the attack occurred adjacent to a 15-story AT&T service center building, it could represent the first time that a critical infrastructure facility was deliberately targeted for an attack against a tall building. Because VBIEDs might also carry a chemical, biological, or radiological (CBR) weapon, some security departments have also deployed surveillance cameras to monitor access to exterior and interior air intakes.

CBRs and viral weapons are an increasing concern given the coronavirus pandemic's ability to upend most of the world and cripple economies with what started as a failure to properly contain, quarantine, and treat initial carriers.
Whether motivated by personal reasons, a psychological imbalance, or terrorist or political agendas, these attacks mean that security departments must prepare countermeasures for a spectrum of assaults.

Mitigation Measures
While the attacks mentioned above highlight past incidents, security is not solely about learning from mistakes—it also involves mitigating emerging risks.

For example, a future attack on a tall building might involve the use of a weaponized unmanned aerial vehicle to assault employees, residents, or property on both the top and ground floors. Given the escalation in political polarization in the United States and other countries, a worst-case scenario postulates violently militant elements hiding among civil protestors until they vandalize buildings' street-level establishments by smashing their windows, looting merchandise from retail stores, setting fire to the premises, and trying to break into the buildings' entrances and attack office personnel.

High-rise building owners should therefore also consider the types of retail stores that might lease space on the ground level and the level of security required to protect them from potential threats. Owners should also consider what might occur if a unit on a building's ground floor is targeted to damage the entire floor or the building's overall structure.

Beyond orchestrated physical attacks, the COVID-19 pandemic presents another potential threat. Perpetrators—disgruntled employees, former employees, or terrorists—infected with the coronavirus or another pathogen could intentionally target iconic buildings with the goal of generating massive publicity and panic.

Because tall office buildings are considered potential hotbeds of viral infection, this could result in massive infections, economic damage, and insurance liability costs to properties' owners and managers. The publicity would create another wave of damage as companies and managers attempt to regain public trust in the facility.

For these scenarios and others, an **enterprise security risk management (ESRM)** process can mitigate the likelihood of a spectrum of potential attacks against tall buildings. At its most basic level, risk is determined by the potential or probable threat, vulnerability, and consequence of a scenario.
Analysts can operationalize risk through an actuarial quantifiable methodology, with overall risk scored on a scale of 1 to 100 and based on the scores of each component. With regards to the threat, it is crucial to identify the types of threat actors that might target a building, ranging from terrorists to malevolent infectious disease spreaders; attack capabilities; and local presence. The degree of vulnerability is assessed according to factors such as security systems and target hardness. Finally, the extent of consequence of an attack is based on factors such as estimated casualties, property damage, and financial, insurance, and legal damages from an attack.

THE CONSEQUENCE OF AN INFECTIOUS ATTACK AGAINST SUCH FACILITIES MAY RESULT IN FEWER CASUALTIES THAN IN PREVIOUS YEARS, BUT THE COST OF REPAIRING AND SANITIZING A BUILDING'S FACILITIES AND REPUTATION WOULD STILL BE RELATIVELY HIGH, INCLUDING THE RELUCTANCE OF EMPLOYEES TO RETURN TO SUCH FACILITIES.

For office buildings currently experiencing a low level of occupancy due to social distancing requirements, the consequence of an infectious attack against such facilities may result in fewer casualties than in previous years. But the cost of sanitizing a building's facilities and repairing its reputation would still be relatively high, including addressing the reluctance of employees to return to such facilities for a lengthy period.

Security leaders should be ready to take the knowledge gleaned from a risk analysis and implement it into learning and practice programs for teams.

"Having emergency policies and procedures, as well as business continuity plans, in place is crucial—not just a check-the-box guide, but thoughtful, thorough manuals that are specific to a company and its facilities," says Malique Carr, psychologist and vice president at risk mitigation firm TorchStone Global. "It can be very hard to detail out every nuanced scenario. Therefore, it is important to train employees how to proactively think about risk and risk mitigation."

Carr also recommends against letting building employees wait until an emergency or attack—full of chaos, alarms, dust, or debris—to figure out potential exits or determine if there is sufficient personal protective equipment.

"Investing time and funds into training employees to enhance situational awareness, emergency preparedness, and empower them with the tools to quickly make informed decisions and actions to mitigate risk is key," Carr says.

Finally, utilizing protective intelligence resources will enable security personnel to be informed about emerging threats nearby or directed at a company, its key stakeholders, and its buildings and facilities.

As with other arms races, previous attacks have provided terrorists, active shooters, and other threat actors with greater opportunities to learn how to circumvent security enhancements, increasing the likelihood of a successful attack against tall buildings. This evolutionary process will continue as both attackers and security departments learn from the past to upgrade and improve their respective missions.