11 Best Practices for Crisis Preparedness

*At the 2021 OSAC Annual Briefing, Ambassador Michele Sison, now Assistant Secretary of State for International Organization Affairs participated in a panel on amorphous threats. During the panel, she gave an informative list all security managers should take while preparing for the possibility of insecurity abroad. Although the exact responses to a terror attack may differ from that of a kidnapping, a protest that has turned violent, a natural disaster, or any other type of potentially dangerous situation, the steps Amb. Sison laid out are ideal boxes for security managers of any size organization to check when preparing for emergencies involving their personnel, facilities, or operations. The overarching themes are **preparation** and **communication**. After all, many times the most mundane of administrative actions and the simplest personal interactions can mean the most in a time of crisis.*

Best Practices

Preparation

1. Physical Accountability
2. Practice Makes Perfect
3. Temporary Hideouts
4. Avoiding Predictability
5. Take Advantage of Available Resources
6. Prepare for the Extreme

Communication

7. Reach Your Personnel…
8. … And Their Families
9. Relationships = Information
10. Keep Your Ears to the Ground
11. Alternative Methods of Communication

Preparation

1. Physical Accountability

It may sound exceedingly simple, but do you know where your people are? Sure, you know where your employees work, and you might know where they are while they're traveling on business. But what about after work, on weekends, on personal trips away. Do you have a personnel locator system? Especially for employees abroad, this can be of paramount importance. In the case of an emergency, you don't want to have to worry about trying to account for people who aren't in an affected location. Develop and maintain a system to account for the whereabouts of your people, and ensure they keep the system up to date. Everyone for whom you are responsible while they are abroad should at least tell you every time they are away from their station; you decide where that distance threshold should stand.

2. Practice Makes Perfect

Drills are so important. We run fire drills in elementary school, but do we run drills for more complicated emergencies in a professional setting? Practice makes perfect, and emergency drills are no different. Think about all the potential emergencies that might affect your workplace: natural disasters, criminal issues, terror attacks, utility failures, personnel medical emergencies. Make sure the drills focus on differences between the emergencies and account for all possibilities based on local variables; fire drills should look and feel different than active shooter drills. Develop realistic and simple reaction plans, and run regular and mandatory drills with your entire staff; everyone from new hires to the CEO needs to participate, and nobody should know when they might happen.

3. Temporary Hideouts

Think about those various emergencies, and figure out how best to incorporate safe haven locations in your facilities and in your personnel's homes. This doesn't have to mean bullet-proof safe rooms—though it could! Is your housing in a flood-prone region? Make sure there is easy access to a higher story. Do your offices have windowless rooms with reinforced doors in case of an active shooter or other intruder? And is there a phone in that room? You might already walk around your facility looking for potential security vulnerabilities, but make sure you take housing into account as well, especially if you have a duty of care to your international staff.

4. Avoid Predictability

By now, avoiding time and place predictability should be a standard SOP for anyone in an environment prone to insecurity, right? But we all tend to fall into routines, and switching things up isn't easy. While managers can ask personnel to maintain personal security by using different routes and visiting different locations, what can organizations do to build that into their overall plans? How about staggering work schedules so there aren't bottlenecks at the exits? How about offering remote work so employees don't have to commute through a potentially problematic environment every day? Avoiding time/place predictability isn't just about physical security, either. Just as a terrorist might take advantage of predictability, so would someone intent on stealing information from someone who uses the same café wi-fi every morning or takes a work call on a stroll through the same park every afternoon.

5. Take Advantage of Available Resources

The U.S. Government—and other governments around the world—has prioritized the safety and security of its nationals abroad. But even the best programs need participation to be effective! Security managers need to impress on their international staff the importance of registering with programs like the Smart Traveler Enrollment Program (STEP), which gives U.S. nationals abroad instant notification of security alerts from the nearest U.S. embassy or consulate. Managers themselves should register as OSAC members to get access to the most relevant and timely security information, not to mention an office of security analysts and program managers ready to help. While your third-country national employees' home governments might have programs like STEP, they should at least have the emergency contact information for their nearest embassy or consulate programmed into their phones.

6. Prepare for the Extreme

Drawdowns and evacuations can be fraught processes for even the most prepared institutions, but they can be especially difficult for personnel who must uproot their lives—and possibly those of their families—to leave their location in an instant. Once you draw up organizational tripwires and SOPs, ensure you communicate them effectively to your personnel. Explain to locally employed staff how they are (or might not be) involved. What happens to pets during an immediate evacuation? Do you have a travel agency located outside of the country available to ticket passengers to leave on short notice, in case insecurity makes domestic ticketing impossible? Will staff be reimbursed if they have to pay their own way out due to organizational mandate (or if they choose to do so despite the lack of one)? Have you prepared for contingencies by securing visas for neighboring countries in case the best way out of an emergency is a road convoy?

Communication

7. Reach Your Personnel...

Sometimes, old-school solutions stick around because nothing better has come along to supplant them. There may be plenty of technology that appears to make the old phone tree system obsolete—think email distribution lists and listservs, robo-calls, or telephone apps—but often these solutions to information sharing dilemmas have single points of failure. What if the electricity or internet goes out? What if the person charged with starting the whole process is out of commission? Don't make one person or one program account for everyone. Institute a simple phone tree to get the word out, especially in areas prone to technology/utility failure, and don't forget to program numbers into your cell phones. Even when phone trees don't work, it's easy to work backwards to find out where the break in the chain exists.

8. … And Their Families

You've drilled plans with your employees, you've noted where your employees are traveling, you've updated them on the latest threats. But are you talking to their family members? Don't forget that many of your personnel might be in-country with their families, who may have very different experiences than your employees. A spouse might work for a local organization, which might not see security the same as an international organization would; will they know where to evacuate in case of emergency weather conditions? Kids going to school might experience insecurity while their school bus is en route, like protests that stop traffic; do they know what to do in case a march turns violent? Develop materials for family members of various ages and situations, and offer them not only to your international employees, but to your local staff as well.

9. Relationships = Information

What is your relationship with local law enforcement? (You do have a relationship with local law enforcement, right?) Even in an area with a capable and responsible police force, it can only help to have a working relationship with the professionals that might be your first line of defense if things go wrong. Meet with local police officers and other relevant agencies to explain your situation, your potential needs, and your security concerns. Explain to them why your presence is beneficial for the community; find out if you need to supplement their capabilities with some (more) of your own. Set up a healthy line of communication between your shop and the local police so they can easily contact you when the security environment is taking a turn for the worse. And make sure your communication goes two ways: report incidents, lend a hand when you can, and be a good neighbor.

10. Keep Your Ears to the Ground

Police know the beat, but so do civilians. What other ways are there for you to find out local security information? Set up social media alerts hooked to local sources and tagged for local issues. Create wider searches for overall environmental shifts, but personalize searches to keep abreast of more granular changes in the neighborhoods around your facilities and lodging. Don't overlook social and traditional media sources in a local language, and make sure you have a local employee on your staff with their ears to the ground. You may not be the very first to know when the winds shift, but you certainly don't want to be the last.

11. Alternative Methods of Communication

How do you keep in touch with your staff? Do you call them on their cell phone, or text them? Or do you email them, or maybe use WhatsApp or Twitter? Great! You likely know the best way to get information to your people. But consider changing all of those ORs into ANDs! Keep current lists of phone numbers, addresses, work and personal email addresses, and anything else that will help you reach your personnel in an emergency. And what if an emergency hits when someone has forgotten to charge their phone, or mobile service is cut? Think about two-way radios, satellite phones – and even land lines -- as secondary or tertiary ways to get information in or out during an emergency. Redundant communications are incredibly important if a storm knocks out cell towers, if an app's servers go down, or if a local government disables certain forms of communication. But they could also be good if your employee switches cell carriers (and phone numbers) without remembering to tell the office. Redundant communications will not only help your emergency planning but your administrative messaging as well.

Additional Information

OSAC offers dozens of reports focusing on security best practices for many different scenarios – from kidnapping and earthquakes to passport loss and road safety – in its Traveler Toolkit, available online without an OSAC password required. OSAC analysts can also help you plan for whatever insecurity lies ahead, including providing you with resources and contacts wherever your operations take you.