HOW TO SPOT THE WARNINGS

Firestorm has aggregated best practices and research from many sources, including the U.S. Secret Service, FBI, OSHA and other thought leaders, on the topic of workplace and school violence. This research serves as the foundation for the Behavioral Risk and Threat Assessment program, which Firestorm calls BeRThA®.

WHAT IS BERTHA?
The underlying premise of BERTHA is that individuals who commit acts of violence exhibit warning signs long before they become violent. The goal of BERTHA is to make everyone aware of what those warning signs are, how to report them and what your organization should do with the information once you get it.

BERTHA HAS SEVERAL CRITICAL COMPONENTS

AWARENESS - Educating everyone in the organization on not only what constitutes a “threat,” but also what constitutes “behaviors of concern.”

REPORTING - Providing everyone with a means to report what they see or hear, including through an anonymous reporting tool (text, mobile app, voice call, web form).

CENTRAL REPOSITORY - All behaviors and threats are not equal, but each represents a data point: a dot that, if connected to other dots, presents a picture of someone who may be on a path to violence. It is important that all reports be aggregated in a central repository so that those charged with responding, investigating and analyzing the seriousness of a situation have a means of gathering all available information about a subject.

BERTHA PLAN

Upon receipt of a reported threat or behavior of concern, the BERTHA plan is activated. The BERTHA plan sets forth the steps a designated and trained multi-disciplinary Threat Management Team (TMT) within the organization will follow:

+ INVESTIGATION
  The investigation process should document the incident/threat or behavior of concern and gather information, resulting in an initial threat-level determination.

+ BEHAVIORAL RISK SCREENING
  Depending on the threat level, a behavioral risk screening should be conducted. The TMT should make a determination as to whether the subject poses a guarded, elevated or severe risk.

+ ACTION PLAN
  Following every investigation or screening, an action plan for short or long term intervention should be documented and implemented by the TMT.

+ MONITORING PLAN
  Upon determination of the action plan, the TMT should make arrangements for supervision and monitoring of the subject’s behavior.

+ SIGN-OFF AND RECORD KEEPING
  All forms should be signed by participating TMT members and filed in the Central Repository.
HANDLING AN INTRUDER

ALICE Training Institute provides life-saving mental and physical tools for those who may experience a violent, life-threatening situation. The program is specifically designed so that anybody can employ the strategies: male or female, young or old. ALICE is an acronym for:

**Alert** and notify authorities and those in harm’s way of the danger at hand. It is important to be as clear and accurate with the information as possible. Remember to identify yourself, your location, the suspect information, type of weapon, direction of travel and a call back number. Don’t hang up unless your safety is compromised or you are directed to by the dispatcher.

**Lockdown** or shelter in place. By locking down and barricading entry points, you are making yourself a hard target and creating a stronghold that nobody should be able to enter. Only police personnel may enter a locked-down room.

**Inform** with real-time updates. This can be accomplished with things such as video surveillance equipment or public address systems. Updates during a violent intruder incident allow you to make sound decisions about how to react and what steps, if any, to take next. They can also distract the intruder.

**Counter** the attacker only as a last resort. There have been instances where victims did not have the ability to lockdown or get out because the violent incident occurred right next to them or they were in an area that was not securable. There is also the possibility of the intruder breaching a secured area. If this is the situation, then total commitment to countering the attacker is essential. Use assorted objects as distraction devices, spread out, turn out the lights and be ready to cause confusion for the intruder and make yourself a hard target.

**Evacuate** or get out!! Your goal here is to put as much time and distance as possible between you and the attacker. Don’t use the same rally point you use for a fire or earthquake drill. You want to move much further away from this danger zone. Remember, there are no guarantees in an active shooter/violent intruder situation, but the more you prepare, the better your chances of survival.
COMMUNICATING DURING A CRISIS

IN THE EVENT OF A CRISIS, WHAT SHOULD YOU DO?

**Determine** who is in charge. CEO? Board member? That person must give clear direction.

**Ask** yourself “why” five times before every communication. “Why now?” “Why contact the media?”

**Know** that most of what you learn in the first 24 hours will be wrong or factually incorrect.

**Document** media calls, but do not return the calls.

**Make** sure all employees know there is only one spokesperson. Provide employees (who are not spokespersons) a talking point: “I am not an authorized spokesperson for the company. I would be happy to take your information and pass it on.”

**Anticipate**, in the event of injuries/fatality/criminal act, that first responders will take control of scene.

**Determine** who will interface with first responders.

**Stick** to themes, home bases and message maps.

+ **We will not be defined by this event.**
+ **We will invent the future.**
+ **We will embrace the victims.**

**Develop** a “victim” strategy. The victim’s family has a huge impact on the overall consequences your organization will suffer.

+ **Appoint** 24/7 family representatives. Have backups.
+ **Clear** all communications with the victim’s family, whenever possible. If the family does not want you to discuss the situation, that gives you basis for not releasing early communications.

IN THE EVENT OF A CRISIS, WHAT SHOULD YOU AVOID?

**DON’T** talk through the media or communicate through a third party. Communicate directly.

**DON’T** give phone numbers, dates or times. Don’t fall into a numbers game.

**DON’T** put anything in writing. Meet face to face or telephonically if possible. (This recommendation does not apply to life-safety situations.)

**DON’T** explain. When you are explaining, you are losing.

**DON’T** forget someone important (donor, regulator, shareholder). Identify ALL constituents.

**DON’T** turn over any documents/computers (to law enforcement, etc.) until directed by counsel.

**DON’T** take ownership of someone else’s grief.

**DON’T** characterize someone else’s feelings or what the loss must mean to that family.

**DON’T** talk about how the loss/incident makes you feel. No word you choose will measure up to what the family would expect you to say. Instead, focus on the family: “Our thoughts and prayers are with the family.”

**Don’t** reply to anything on social media, at least initially.