Workplace Violence Prevention: Identifying Behaviors of Concern with Predictive, Actionable Intelligence

April 2016
By Karen Masullo for Firestorm

Prior to my current career, I worked in the career transition industry. While the delivery model has changed, the basic deliverable of career transition is to assist employees in their transition out of current employment. These transitions may be a result of restructuring, merger and acquisition activity, downsizing of operations, a reduction in force, or performance related separations.

As with any employment separation situation, and while each situation is nuanced by the people, culture and climate involved, emotions and stress levels run high. It is a reality of the workforce lifecycle that even those situations perfectly managed can result in threats or incidents of violence.

Forewarned is Forearmed

How many times – after a transition related workplace violence event – have we read news that describes missed behavioral signals, the "cry for help" expressed beforehand by a perpetrator?

We know that workplace safety is front and center in the minds of all boards of directors, senior leadership, management and employees, vendors and customers. More than 2,000,000 acts of violence are reported annually, with incidents ranging from verbal threats to the use of weapons and physical violence.

While there is no definitive behavioral truth, many perpetrators of workplace violence exhibit common warning signs and behaviors of concern long before they act violently. These warning signs – Predictive Intelligence – may appear in several ways:

- Warning signs detected early such as in the hiring process itself;
- Warning signs observed over time to include changes in behavior or observed 'behaviors of concern' by fellow employees and supervisors;
- Warning signs shared via technology such as behaviors detected through the monitoring of public social media posts and conversations. Behaviors may surface through structured intelligence around keywords, keyword phrases, images, videos and emojis, and meta- and geo-information.

To make a workplace and the people in it safer, a prevention program must focus on just that: preventing the act of violence in the first instance. The implementation of a complete Workplace

Violence Prevention Program incorporates threat detection capabilities, or Predictive Intelligence, related to behaviors of concern.

While behaviors of concern are not limited to only shared, social or technology-based interactions, these types of applications do allow us early warning in a way that did not exist in past decades. Predictive Intelligence then, includes the analysis of publically shared, aggregate and individual user-driven social intelligence in addition to live, face-to-face observations.

A challenge for many organizations however is in who owns social media and other monitoring in the organization.

Many in an organization may be of the mindset that social channels are 'owned' by Marketing and as such, Marketing will flag and escalate behaviors of concern as a simple, extra task added to their job description.

Misassignment to an entry-level role, the responsibility for social media management is a sign that an organization does not understand the associated risks of inexperienced social media management. Likewise, assigning Predictive Intelligence to Marketing Teams is unfair to Marketers who are trained to engage. This added duty puts them in a position for which they are unprepared, keeps them from their primary focus and role, and may actually escalate or aggravate a potentially violent situation. It is additionally irresponsible to assign analysis to employees untrained in investigative work as constant exposure to negative and threatening images and content can create psychological and emotional fatigue.

Predictive Analytics requires specific training in specific skills:

Risk Assessment: Persons trained to conduct complete risk assessments on specific users to determine the risk level associated with certain individuals of interest.

Situational Awareness: Training in the identification, processing and analysis of critical information communicated across various social media networks.

Complex Link and Relationship Analysis: Training in understanding how to visualize an individual's social activity to assist in identifying communities, inferring demographics and understanding relationships and conversations.

Understanding Syntax and the Elements of Language: Comprehension of the syntax and context of language; analysts must understand the difference between song lyrics, idle conversation or a true potential threat. Training must address the cultural environment with data intelligence needs.

Tools and Application skills may include:

Location Analysis: The ability to identify activity relevant to an organization, its facilities or campuses based upon location-specific intelligence.

Social Reenactment: Logical situational analysis and decision-making that allows the development of historical queries to recreate an event in time from a social perspective to find potential witnesses, suspects, or other insights.

Intelligent Data Mining: The ability to Intelligently gather, sort and filter billions of social posts daily to specifically target and identify only the posts relevant to an organization's scope of interest.

Just as in live, face-to-face situations, technology-based threat assessment professional training should include a roadmap for an inquiry or assessment related to a social media threat. Questions may include:

1. What are the subject's motive(s) and goals?

2. Have there been communications suggesting ideas or intent to attack?

3. Has the subject shown inappropriate interest in:

    - previous attacks or attackers;
    - weapons (including recent acquisition of any relevant weapon);
    - incidents of mass violence (terrorism, workplace violence, mass murderers).

4. Has the subject engaged in attack-related behaviors? These behaviors might include:

    - developing an attack idea or plan;
    - making efforts to acquire or practice with weapons;
    - casing, or checking out, possible sites and areas for attack;
    - rehearsing attacks or ambushes.

5. Does the subject have the capacity to carry out an act of targeted violence?

6. Is the subject experiencing hopelessness, desperation and/or despair?

7. Does the subject have a trusting relationship with at least one responsible adult?

8. Does the subject see violence as an acceptable, desirable, or only way to solve problems?

9. Is the subject's conversation and "story" consistent with his or her actions?

10. Are other people concerned about the subject's potential for violence?

11. What circumstances might affect the likelihood of an attack?

12. Do social postings indicate:

    - The loss of a personal relationship
    - Financial loss
    - Legal action
    - Loss of face or humiliation
    - Significant personal rejection

When creating the Predictive Intelligence aspect of a Behavioral Analysis program, organizations must discuss how to balance people, systems and technology-based solutions with a socio-cultural approach to threat detection and mitigation. As part of this discussion, it is incumbent upon teams to determine the appropriate level of effort including investment required to deploy sufficient resources to detect activity, and the reliability and quality of the prediction capability that can be achieved.

By using Predictive Intelligence, organizations may determine if there are looming threats, especially during high stress events such as restructuring and employee separation. Through the combination of Predictive Intelligence tools with seasoned, experienced practitioners, approaches can be implemented that identify what is being said in social and traditional media in real-time, not hours or days later. Through the combination of leading Predictive Intelligence with seasoned, experienced practitioners, lives can be saved. The application of experience in combination with the identified risks, threats and vulnerabilities provides Predictive, Actionable Intelligence.

Karen Masullo, Firestorm.com

Karen Masullo is Chief Intelligence Officer and EVP of Business Intelligence for Firestorm. In addition to serving as Firestorm's own in-house social media advisor, she also serves on the Firestorm Solutions Expert Council and delivers social media strategy and policy services for Firestorm clients.

kmasullo@firestorm.com

Learn More about Predictive Intelligence approaches for your organization More >>>