From the Guest Editor: Understanding Targeted Violence

Russell Palarea, Ph.D.
Consulting Operational Psychologist (CTR), Office of Protective Intelligence Investigations
Diplomatic Security Service, U.S. Department of State*
President, Association of Threat Assessment Professionals

Understanding why people commit targeted violence attacks and how to prevent them has become an increasingly urgent issue over the years. Whether it's a mass shooting, mass stabbing, mass vehicular attack, chemical/biological weapon, or explosive device, the commission of targeted attacks have reached public health epidemic proportions. Despite the founding of the Association of Threat Assessment Professionals (ATAP) in 1992 (www.atapworldwide.org), creation of the U.S. Secret Service's behavior-based threat assessment model in 1995 (www.secretservice.gov/data/protection/ntac/tatv95.pdf), and current practice of threat assessment across the Federal Government, state/local agencies and communities have been slow to adopt its practice.

While attacks are committed by both insiders and outsiders, those committed by insiders afford coworkers and supervisors the opportunity to observe the concerning behavior escalating over time, and thus implement threat management strategies to prevent the attack. The current proliferation of Insider Threat Programs across the Federal Government, Government contractors, and the broader corporate community brings new opportunities for implementing behavior-based threat assessment programs. Although Executive Order 13587 was originally created to protect classified information, the 2012 Presidential Memorandum expanded insider threat programs to preventing acts of violence against the Government or Nation. This merger of the information disclosure/espionage prevention and violence prevention missions is critical.

From a human factors perspective, disgruntled employees have a spectrum of harmful acts at their disposal: they can shoot/stab/run over coworkers, set off a bomb at the worksite, sabotage mission critical equipment, launch a cyberattack, disclose classified information, or commit espionage. The use of the behavior-based threat assessment model to identify, investigate, and assess pre-attack behavior, and then mitigate the attack, is the solution to preventing these acts of harm and violence.

In this edition of **The Insider**, you will hear from threat assessment experts with the U.S. Secret Service National Threat Assessment Center, FBI Behavioral Threat Assessment Center, University of Nebraska Public Policy Center, University of Virginia Youth Violence Project, and the VA Hospital Behavioral Threat Management Program, on using behavior-based threat assessment models to prevent violent attacks. Thank you to the editorial staff for dedicating this edition of **The Insider** to this critical aspect of the insider threat mission.

*The views expressed in this article are those of the author, and do not necessarily reflect those of the U.S. Department of State or the U.S. Government.