ACTIVE THREAT INTELLIGENCE DIGEST

KIERNAN GROUP HOLDINGS

FOR AN ANALYTIC AND OPERATIONAL ADVANTAGE

NOVEMBER 2016

WWW.KIERNAN.CO

Welcome to Kiernan Group Holdings' (KGH) *Active Threat Intelligence Digest*. This monthly newsletter will cover topics of interest regarding elements of the active threat phenomenon: ***active shooter incidents***, ***workplace violence***, ***insider threats***, and ***terrorism***, with a focus on planning and prevention.

Source: HRUSA

Workplace Violence: What You Should Know

By Sally Maxwell, Senior Analyst

Workplace violence, one of the four dimensions of "active threat," could happen in any business, organization, school, or municipality. News articles frequently detail shootings, stabbings, and other attacks at places of employment, whether conducted by employees against their colleagues or against them by others, such as criminals or even customers, at their site. In many of these cases, the perpetrators have a grievance against a company, having been reprimanded or fired. In a few cases, ex-spouses of employees carry out attacks against them at their place of business, thereby placing others at risk of injury or death, as well.

Four types of workplace violence exist (see Figure 1 and Table, page 2): Type I, Criminal Intent; Type II, Customer/Client; Type III, Worker-on-Worker; and Type IV, Personal Relationship. In examining workplace violence through a commonly accepted typology, the phenomenon can be analyzed by looking at the type of relationship the perpetrator has with the venue or employee. For example, worker-on-worker violence is an internal threat and customer/client and criminal intent incidents come from outside the organization. Personal relationships, as defined in Type IV, also would be external because the threat comes from outside of the organization.

(continued on page 2)

In this Issue...

Workplace Violence: What You Should Know

5 Things To Know about Workplace Violence

Modeling the Pathway to Violence

Active Threat Bookshelf

About KGH

In the Next Issue...

Terrorism as Component of Active Threat

5 Things To Know About Terrorism

Active Threat Bookshelf

KGH News...

- *November is Critical Infrastructure Security and Resilience Month, a nationwide effort to raise awareness and reaffirm the commitment to keep our Nation's critical infrastructure secure and resilient. KGH has committed to building awareness of the importance of critical infrastructure. See page 7 for more information.*
- *KGH has been selected by DHS to deliver 70 Active Shooter Preparedness Workshops in FY17. See* www.govevents.com *for more detail.*

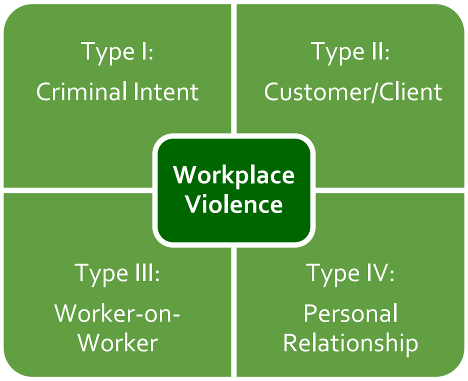


Figure 1: Four Types of Workplace Violence

The source of the threat, therefore, provides challenges for prevention. External threats can be mitigated somewhat by limiting access to the facility through the use of key cards or other security measures. Internal threats, however, can be much harder to prevent. They require a thorough plan of action to identify, report, and monitor behaviors that might suggest a person is on a pathway to violence (see "Modeling the Pathway to Violence" on page 5).

In a study of 152 fatal shootings attributed to workplace violence, KGH analysts determined that 68 percent of these events were committed by workers on other workers—presenting an inside threat that can be difficult to prevent. With planning and preparation, however, at least some of these threats can be mitigated or even prevented, especially with an understanding of a potential attacker's pathway to violence.

(continued on page 3)

Type	Description	Example
Type I: Criminal Intent	A person who has no relationship with the venue or its employees commits a violent crime, such as holding up an employee in a burglary or shooting.	In an armed robbery in 2012, O'Brian McNeil White entered the J.T. Tire store in North Carolina and demanded money from the cashier. While she was taking money from the safe, White fatally shot her and another person, then wounded two others before he was arrested.
Type II: Customer/Client	An employee's customer or client becomes angry as a result of his or her perceived grievances that he or she attacks the employee. This type of workplace violence occurs in certain professions, such as healthcare, law enforcement, corrections, retail, and finance.	In 1999, Dung Trinh entered West Anaheim Medical Center and opened fire, killing three hospital workers in retaliation for what he perceived to be inferior medical treatment provided to his mother, who had died earlier that morning.
Type III: Worker-on-Worker	Type III, or worker-on-worker violence, consists of attacks against coworkers, usually by disgruntled employees or former employees. Frequently, this is manifested through employees who may hold a grudge against a supervisor for conducting disciplinary actions against the employee, including suspension or termination.	In 1997, Hastings Wise drove to R.E. Phelon Company, a lawn mower parts manufacturer from which he'd been fired several weeks earlier. Hastings arrived during shift change and shot a security guard before fatally shooting the supervisor who had fired him. He also targeted workers in a department where he had hoped to work and killed a woman who had received a promotion to another position he had wanted.
Type IV: Personal Relationship	Type IV involves an incident in which someone having a personal relationship with an employee, such as an ex-spouse, commits a violent act against the employee and possibly others at the target's place of work.	Usually this is a domestic incident that spreads to bystanders. In 2012, Radcliffe Haughton entered the Azana Day Salon in Brookfield, Wisconsin, where his estranged wife worked. He fatally shot her and two coworkers and wounded four others before killing himself.

Threat to Organization Safety and Sustainability

Fatal workplace violence incidents have declined in the past decade, but they continue threatening the safety and livelihoods of many employers. In 2014, the latest year for which data are available, eight percent of fatalities in the workplace were caused by homicide, according to the Bureau of Labor Statistics. The rate of workplace fatalities declined steadily—but not significantly—between 2006 and 2014 from 4.2 fatalities per 100,000 workers to 3.4. Yet, certain recent workplace violence incidents, such as former Major Nidal Hasan's 2009 attack at Fort Hood, in which he deliberately targeted his fellow military personnel, and Omar Mateen's attack against the Pulse Nightclub, in which several of the club's employees were killed or wounded, highlight the prevalence of workplace violence incidents as a major concern.

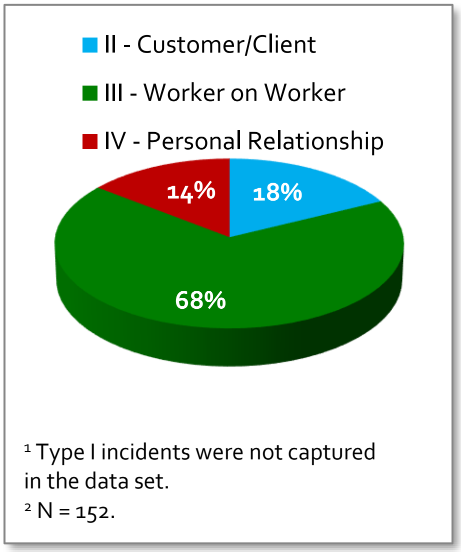
Although OSHA has issued general guidance to employers about preventing workplace violence, it does not require employers to comply with the guidance. OSHA's General Duty Clause, which requires employers to provide a safe work environment, is interpreted by OSHA to mean that an employer has a legal obligation to provide a safe workplace; however, employers are not strictly liable under the statute, according to the American Bar Association.

Still, civil lawsuits can present a major financial burden to companies, organizations, and municipalities. For example, the family of a victim of the 2015 shooting at San Bernardino's Inland Regional Center filed a lawsuit claiming damages of more than $200 million against the county, which runs the facility.

Disgruntled Employees Pose Biggest Threat

Two-thirds of workplace violence is worker-on-worker, according to the KGH study, leaving businesses and organizations of all sizes and sectors vulnerable. Most of the incidents examined in the study include a disgruntled employee taking out his or her grievance against supervisors, usually after a disciplinary action has been taken against the employee. In many cases, the employee has left the premises and returned with a weapon; in others, the employee has come to disciplinary meetings already armed. In at least one incident in the study, a fired employee returned and fatally shot the security guard, who had been informed to watch for him, to gain entry to the building and kill his former supervisors. The necessary access provided to these individuals, even when limited, exacerbates the challenge in preventing such violent actions.

Figure 2: Percent of Workplace Violence by Type, 1966-2016



[1] Type I incidents were not captured in the data set.
[2] N = 152.

Many sectors, too, are vulnerable to workplace violence. More than half of workplace violence shootings occurred in the Commercial Facilities Sector, according to the KGH study, making those companies most susceptible to violence. Nineteen percent of fatal workplace shootings in the study occurred in the Government Facilities Sector, mostly targeted at judges and social workers who delivered adverse findings, such as custody arrangements, against eventual perpetrators. The Critical Manufacturing Sector saw 12 percent of the workplace fatalities, the third highest-ranking sector. All workplace violence incidents in this sector were Type III: Worker-on-Worker.

Planning and Preparation Can Reduce Risk

With effective planning and preparation, companies can reduce their exposure to workplace violence. Emergency plans should include preparations for active shootings, stabbings, and other physical threats in addition to the typical concerns of fire and theft. These plans should be comprehensive, widely disseminated, and regularly exercised.

In addition to developing emergency response plans for workplace violence, implementing threat assessment teams throughout the organization can mitigate or prevent acts of violence. Teams that include representatives from first-line management, human resources, and security work together to identify, assess, and manage at-risk employees and their behaviors on the Pathway to Violence. Including such teams in a corporate security strategy was endorsed in 2011 by the American National Standards Institute, a private, not-for-profit organization that develops voluntary, consensus standards for products, services, processes, systems, and personnel.

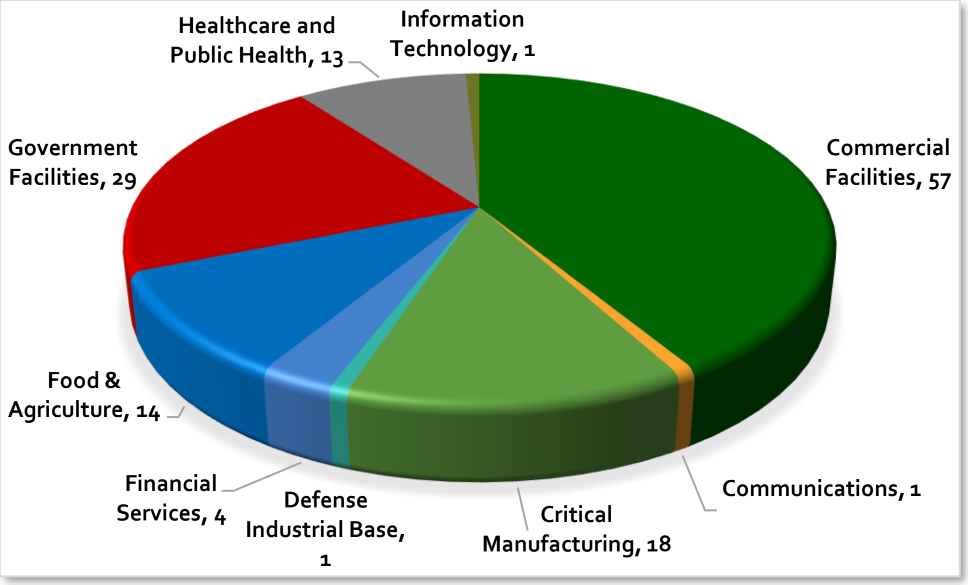
Additional Resources about Workplace Violence Prevention:

Bureau of Labor Statistics: *Census of Fatal Occupational Injuries*

Centers for Disease Control and Prevention: National Institute for Occupational Safety and Health

US Department of Homeland Security: *Violence in the Federal Workplace: A Guide for Prevention and Response*

Figure 3: Fatal Workplace Violence Shootings by Sector, 1966-2016



5 THINGS TO KNOW ABOUT WORKPLACE VIOLENCE

#1
Workplace violence can be perpetrated by people from the outside (clients, relatives of employees, or criminals) or from the inside (employees or ex-employees).

#2
More than two-thirds of workplace violence incidents in a recent study (see Figure 2) were committed by employees or ex-employees.

#3
Ninety percent of fatal workplace violence shootings in a KGH study occurred in three sectors: Commercial, Government, and Critical Infrastructure.

#4
Prevention of both internal and external threats should be part of your organization's planning.

#5
Many workplace violence threats can be mitigated through preparedness and prevention before grievances turn into action.

FAST FACTS

Nearly 90 percent of workplace violence incidents in a database of 152 active shooter events occurred in just ***3 of the 16*** Critical Infrastructure Sectors.

Commercial

57

Percent of workplace violence incidents occurred in the Commercial Facilities Sector, 1966 – 2016. Nearly two-thirds of these were Type III: Worker on Worker.

Government

19

Percent of workplace violence incidents occurred in the Government Facilities Sector, 1966 – 2016. Most of these events were targeted against judges and social workers who had delivered judgments against the shooters. Shootings at post offices also fall into this category.

Critical Manufacturing

12

Percent of workplace violence incidents occurred in the Critical Manufacturing Sector, 1966-2016. All workplace violence incidents in this sector were Type III: Worker on Worker.

Modeling the "Pathway to Violence"

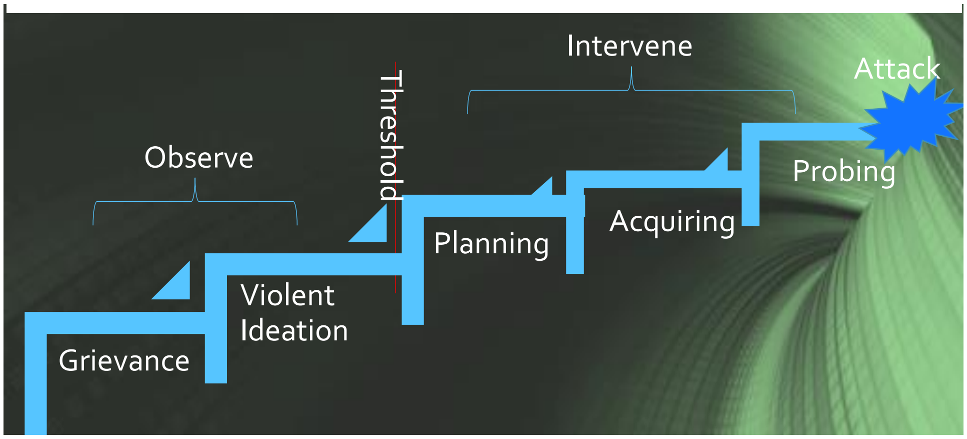
By Thomas Schiller, Dr. Joshua Sinai, and Amanda Wilmore

In the aftermath of an active shooter attack or other types of mass killings, among the first questions asked are why and how did the killer reach the point where he/she had become so vengeful as to conduct such a horrific rampage? A great deal of social science research has been done on individuals such as Dylan Klebold and Eric Harris (Columbine, Colorado, April 1999), Seung-Hui Cho (Virginia Tech, Blacksburg, Virginia, April 2007), and James Holmes (Aurora, Colorado, July 2012) to try and determine their motivation, family background, psychological makeup, and other factors that contributed to their violent attacks.

What emerged from this research were conceptual models centered around "The Pathway to Violence" (PTV), which is composed of a series of progressively escalating stages along with corresponding risk factors identified in the attacker's mindsets and behaviors characterizing them prior to a violent attack. The PTV frameworks are expressed as a spectrum that generally begin with certain types of events of everyday life and family dynamics that may anger and aggravate an individual. The majority of people affected by such aggravating incidents respond to these aggravations in a nonviolent and socially constructive manner, but some may not be able to do so. These individuals may begin to fantasize about rectifying their perceived grievances through retributive violence. Subsequent stages move the individual closer to the point where he/she carries out an attack.

The stages described in a PTV model are not static. Some risk factors may occur in some of the stages—or not at all. At any point along the pathway, risk-based mindsets and activities that might lead to an attack can also be mitigated by what are called "risk-reducing factors," which include personal coping strategies, the influence of friends and family, professional help, and intervention by law enforcement.

Figure 4: Pathway to Violence

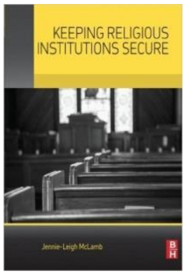


A PTV model is intended to support analysts, administrators, and public safety practitioners by explaining and outlining risk factors that might lead up to an attack. At the same time, however, a PTV model is not intended to be predictive, and may, in fact, be reversible, whether through external intervention or if the potential attacker decides to change his mind. A PTV model might provide insight into intervention points that those associated with a susceptible individual can identify and use to preempt or prevent continued progression along the pathway to violence.

A PTV model that captures "trigger" events that may set an individual on the pathway to violence, as well as delineating a threshold point through which an individual crosses from risk-based mindsets to potentially violent actions, would add value to existing PTV models. Another element to be captured on the pathway is temporal: once the threshold to violence is crossed, the time-period between each subsequent stage is likely to be compressed, which increases the need for rapid and effective interventions. A model that captures these risk-based and mitigating elements would serve as a major contribution to modeling pathways to violence.

Active Threat Bookshelf

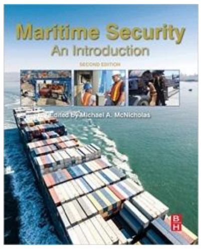
Reviews by Dr. Joshua Sinai



Jennie-Leigh McLamb, Keeping Religious Institutions Secure (Boston, MA: Butterworth-Heinemann/ Elsevier, 2015), 210 pages, $34.95, [Paperback], ISBN: 978-0-12-8011346-5.

With religious institutions under increasing threat by terrorists, active shooters, and other types of threats, this important volume provides highly useful information on security principles and best practices for protecting these 'soft targets' against such attacks. The chapters cover topics such as an overview of the types of threats against religious institutions (such as financial crimes, crimes against property, hate crimes, and homicides); conducting risk assessments (including security surveys); the components of security (beginning with understanding the incident management cycle covering disaster, crisis, and incidents, as well as designing and implementing a physical and electronic protection system); conducting risk assessments (including security surveys); implementing a security awareness training program; identifying and managing individuals who may be 'at risk' for carrying out a violent attack; responding to active shooter events, including protecting children and youth; managing crisis communications and media relations; managing insurance liability issues; and establishing security partnerships with local law enforcement authorities.

The author is a security consultant in emergency preparedness and risk assessments.



Michael A. McNicholas, Editor, Maritime Security: An Introduction [Second Edition] (Boston, MA: Butterworth-Heinemann/ Elsevier, 2016), 528 pages, $106.25 [Paperback], ISBN: 978-0-12-803672-3.

This authoritative textbook presents a comprehensive examination of significant components in maritime security from the perspective of veteran practitioners. The chapters cover topics such as modes of maritime transport; international and U.S. maritime security regulation and programs; security vulnerabilities in the cargo supply chain; targeting and usage of commercial ships and ports by terrorists and criminal organizations; threats presented by maritime piracy and refugee migration; responding to drug smuggling via maritime cargo, containers, and vessels; cyberwarfare threats to seaports and ships; the strategic and leadership components involved in establishing an effective seaport security program; threat mitigation strategies; the need for interagency coordination in responding to maritime threats; and legal authorities for enforcing maritime law, safety, and environmental protection.

There is much to commend in this textbook, including the numerous tables that provide tool kits for maritime security practitioners in areas such as risk management and port security. These include valuable tables of how to conduct risk and vulnerability assessments involving potential security threat scenarios, risk mitigation and mitigation determination worksheets (pages 408-413).

As a textbook, each chapter contains sections on objectives, conclusions, and a summary.

The volume's editor, a former U.S. military and intelligence officer, is the Managing Director of Phoenix Group in Panama and Costa Rica, and Pathfinder Consulting, LLC, in the United States.

***About the Reviewer**: Dr. Joshua Sinai is a Principal Analyst at KGH.*

Keeping Critical Infrastructure Strong and Secure

November is Critical Infrastructure Security and Resilience Month, a nationwide effort to raise awareness and reaffirm the commitment to keep our Nation's critical infrastructure secure and resilient. Safeguarding both the physical and cyber aspects of critical infrastructure is a national priority that requires public-private partnerships at all levels of government and industry.

We know critical infrastructure as the power we use in our homes and businesses, the water we drink, the transportation systems that get us from place to place, the first responders and hospitals in our communities, the farms that grow and raise our food, the stores we shop in, and the Internet and communication systems we rely on to stay in touch with friends and family.

Managing risks to critical infrastructure involves preparing for all hazards and reinforces the resilience of our assets and networks, and staying ever-vigilant and informed. This November, help promote Critical Infrastructure Security and Resilience Month by training your employees on cyber awareness, taking part in the Hometown Security effort, engaging with your community partners or supporting long term investments in critical infrastructure. We all need to play a role in keeping infrastructure strong, secure, and resilient.

To learn more, visit www.dhs.gov/cisr-month.

ABOUT KGH

KGH is a customer-focused, global, law-enforcement and national-security consulting firm that provides ***tailored solutions to complex challenges*** using end-to-end problem-solving approaches focused on information—the raw material of the intelligence and law enforcement professions.

KGH provides operational and analytic expertise by and for practitioners across the homeland security, defense, and intelligence community enterprises. KGH provides analysis for risk identification and mitigation, and to understand the often invisible interdependencies across, between and among all elements of the nation's critical infrastructure and the criticality of public-private partnering to protect and sustain infrastructure against threats, both natural and manmade.