ACTIVE THREAT INTELLIGENCE DIGEST

FOR AN ANALYTIC AND OPERATIONAL ADVANTAGE

APRIL 2017

WWW.KIERNAN.CO

Welcome to Kiernan Group Holdings' (KGH) *Active Threat Intelligence Digest*. This monthly newsletter covers 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: www.ready.gov

In this Issue...

In the Next Issue...

Preparedness without Paranoia™: Empowering People to Respond to Active Threats

By Dr. Kathleen Kiernan, CEO, Kiernan Group Holdings, Inc.

Understanding the modern threat environment does not have to be an intimidating or overwhelming task. From small businesses or organizations to Fortune 500 companies, the resilience of any organization in a threatening situation depends on the extent to which its employees are prepared, confident, and capable of reacting appropriately and effectively.

In this way, KGH's Preparedness without Paranoia™ approach fosters and develops an educated and engaged workforce through teaching heightened situational awareness and increasing each individual's security effectiveness. Specifically, Preparedness without Paranoia™ emphasizes the importance of understanding today's threat environment, recognizing telltale signs of an evolving threat, and empowering people to take effective action.

KGH believes that security is personal and should become secondary in nature, as fundamental as getting ready for school or work or running errands. Personal empowerment—understanding how to respond effectively to acts of violence—changes the threat dynamic by providing options of how to manage a hostile situation.

National models provide universal guidance on actions to take in response to a threatening act. For example, the US Department of Homeland Security's Run, Hide, Fight model provides guidelines and options for responding to threats, but implementing the options varies by person and by situation. In some circumstances, escape may not be immediately possible, leaving the option to hide and/or fight as a last resort. However, not all members of a community are able to run, hide, or fight in a threatening situation because of special and functional needs, fear, or a lack of knowledge about how to react. Hesitance can make a crucial difference in personal survivability of an incident.

Such risk factors can be mitigated through education, preparation, planning, and practice. Preparedness Without Paranoia™ prepares companies and their people with that education through in-person and virtual training tailored to each customer, table-top exercises, and customized security consulting. By training individuals to react according to their capabilities, organizations help ensure survivability and resilience. Making the extraordinary—active threat situations—seem more ordinary shifts the advantage away from an aggressor.

10th Anniversary of Virginia Tech Shooting: Lessons for Resilience and Recovery

By Sally Maxwell, Editor-in-Chief

"April 16, 2007, was a transformative event — not only for the families of the victims, not only for Virginia Tech, but for campus public safety nationally."

- S. Daniel Carter, campus safety advocate, in Collegiate Times

The 10th anniversary of the mass shooting at Virginia Tech University on April 16 recalled the need for universities to have not just plans for preventing such atrocities, but also preparations for recovering from them, should they occur. The Virginia Tech event, in which 32 people were killed and 17 wounded by gunfire, was the largest incident of its kind on a university campus, and it highlighted the requirement for such soft targets to protect its "customers"—in this case, professors, employees, and students and their families—before, during, and after such tragedies.

This wake-up call sparked institutions of higher education to boost their security throughout the risk cycle. One year after the Virginia Tech calamity, *Campus Safety* magazine conducted an online questionnaire of its readers. In the responses, 88 percent said that their institutions had revised or were in the process of revising their campus emergency plans.

Many campuses now arm their police departments, a reaction to the Virginia Tech shooting, said John Roman in 2015, then at the Urban Institute. That year, about 32,000 people worked in campus security, and about half of those were armed, according to Roman. A separate Department of Justice report that same year estimated that two-thirds of universities employed armed officers during the 2011-12 schoolyear in response to pressure from parents concerned about campus safety.

Some states now allow college employees and even students to carry concealed weapons. In Tennessee, more than 500 college and university employees are carrying weapons since a law allowing the practice went into effect in July 2016. In Texas, students were allowed to begin carrying weapons in campus buildings as of August 2016; previous legislation allowed students with concealed carry permits to carry weapons on campus sidewalks, streets, and parking spaces. As of August 2016, eight states allowed students to carry weapons into campus buildings.

Permitting weapons on campus is not the only security change made in response to the Virginia Tech shooting.

Virginia Tech itself has led the way in improving campus security, according to the Collegiate Times. When a university police officer was shot on campus in December 2011, Tech officials notified stakeholders via multiple communication channels—a principal factor of successful emergency alerts, according to Larry Hincker, one of the school's communications officers during the April 2007 tragedy. Tech also implemented threat assessment teams to coordinate warning signs of potentially violent behavior, a model that has been copied elsewhere. These teams coordinate information among various sources—such as professors, administrators, security officials, and behavioral professionals—to identify and mitigate potentially threatening behavior by students.

But even the best-laid security plans cannot stop all threats; therefore, organizations must also plan for response and recovery. For more information, see "Building a Resilient Organization: Effective Recovery from an Active Threat Incident" in this issue.

5 THINGS TO KNOW ABOUT RESILIENCE AND RECOVERY

#1
Developing an educated and engaged workforce through teaching heightened situational awareness increases each individual's security effectiveness.

#2
Risks can be mitigated through education, preparation, planning, and practice.

#3
The Virginia Tech shooting in 2007 highlighted the need for universities to have not just plans for preventing such events, but also preparations for recovering from them.

#4
Resilience can be achieved during the immediate aftermath of an event through effective response and recovery actions.

#5
Recovery tasks can include providing psychological first aid to those affected; managing legal and insurance liabilities; retaining students, business customers, or worshippers; establishing an alternate facility; and regaining reputational branding.

Building a Resilient Organization: Effective Recovery from an Active Threat Incident

By Dr. Joshua Sinai, Senior Analyst

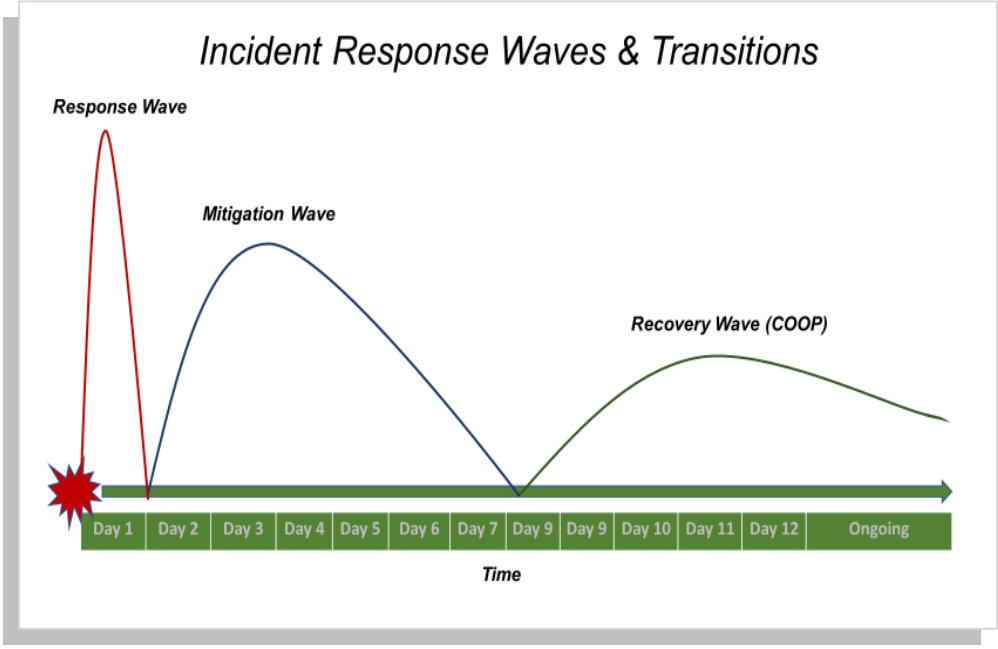
Sometimes, despite an organization's best preparatory and preventative security efforts, it will be targeted by an active threat incident, resulting in loss of life, injuries, and damage to the facility. Staff and employees often are unprepared for the varied stresses and uncertainties that emanate from such critical incidents. To achieve such post-incident resilience, organizations must be able "…to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies." The tasks associated with recovery can include providing psychological first aid to those affected by the incident; managing legal and insurance liabilities; retaining students, business customers, or worshippers; establishing an alternate facility; and regaining reputational branding.

Organizations must be able "…to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."

-Presidential Policy Directive 8, 2011

Such resilience can be achieved during the immediate aftermath of an event through effective response and recovery actions viewed as a series of waves:

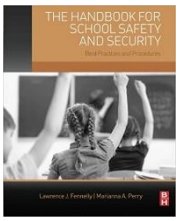
1. **Day 1: Response Wave** – stabilizing an emergency situation in the immediate hours after an attack;
2. **Days 2 to 7: Mitigation Wave** – lessening the near-term impact of the critical incident; and
3. **Days 8 onwards: Recovery Wave** (also referred to as continuity of operations, or COOP) –restoring pre-incident operational functioning and the well-being of those affected by an incident.



Numerous tasks need to be accomplished during the three transitional waves to ensure resilience and recovery. Each wave has its own tasks, and other tasks overlap multiple waves. The key is to have a game plan for each wave, listing each task and assigning them to specific officers in the organization. Many of the tasks have been identified through after-action reports produced by those who have been affected by and recovered from these incidents. The value for the emergency response community will be to identify and provide the sequence of tasks involved in such situations to aid organizations in being better prepared to anticipate and respond to all possible scenarios and shorten their response and recovery time.

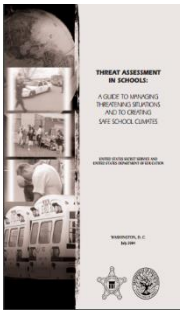
Active Threat Bookshelf

Review by Dr. Joshua Sinai



Lawrence J. Fennelly and Marianna A. Perry, editors, *The Handbook for School Safety and Security: Best Practices and Procedures* (Boston, MA: Elsevier/Butterworth-Heinemann, 2014), 420 pages, $59.95 [Paperback], ISBN: ISBN: 9780128005682.

The contributors to this comprehensive handbook provide a wealth of practical information and procedures for school staffs and administrators to secure K-12 schools against a spectrum of threats, such as active shooters, bullying (including cyber bullying), crimes, vandalism, and hazards (such as dangerous spills from classroom labs). The chapters cover topics such as the types of threats and hazards confronting educational institutions; how to conduct Crime Prevention Through Environmental Design (CPTED) security surveys and assessments; prevention and mitigation methods, including general intruder response guidelines; mass notification requirements in the event of an emergency; procedures for hiring private security services, including liability issues; templates for establishing access control, intrusion detection systems, security lighting, video surveillance technologies, and fire alarms; and the importance of partnering with local first responders and law enforcement agencies. The final chapter presents a listing of "100 Things You Need to Know About School Security." Note: This book differs from the editors' ASIS International volume, reviewed earlier. It has different contributors (although it retains some from the earlier volume) and its chapters are substantially lengthier.



United States Secret Service, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates* (Washington, DC: U.S. Department of Education, July 2004), 60 pages, https://www2.ed.gov/admins/lead/safety/threatassessmentguide.pdf.

This report, which was considered groundbreaking when it was published in 2002, was the product of a collaboration between the U.S. Department of Education and the U.S. Secret Service to examine and prevent school shootings by developing "accurate and useful information about prior school attacks that could help prevent some future ones from occurring." The report was written by a team of top psychologists and school safety practitioners, with several of them working at the U.S. Secret Service's National Threat Assessment Center (NTAC). The report's chapters present a threat assessment framework to predict early warning signs of potential violence, managing a threatening situation, preparing action plans for school leaders to implement a threat assessment program, and utilizing threat assessment as a decision-making tool for school safety.