

AFTER THE MASS SHOOTING IN SAN BERNARDINO, CALIFORNIA, the *New York Times* asked readers if they ever thought about the possibility of a shooting in their daily lives. "The number of responses was overwhelming," reported the paper. "More than 5,000 readers wrote to tell us about the anxiety they felt while riding the subway, going to the movies, dropping their children off at school, and attending religious services."

Such fears soar when those killed are innocent students, whether in elementary school (as in Sandy Hook), high school (Columbine), or college (Virginia Tech). And in one sense, the fear is justified: A 2014 study by the FBI reports that active shooter incidents have, in fact, been increasing in recent years, with nearly a quarter of them occurring in educational environments.

BUT IN ANOTHER SENSE, OUR FEARS ARE MORE EMOTIONAL THAN RATIONAL, more the result of our natural tendency to exaggerate the likelihood of horrific events. According to the National Center of Education Statistics (NCES), "For young students, the risk of homicide was far greater outside of schools. Only one percent of youth homicides took place at schools in 2011-12." Overall, between 1992 and 2012, the number of student, staff, and nonstudent school-associated violent deaths at schools remained relatively steady (fluctuating annually between a low of 34 and a high of 57) and dropped slightly for children aged 5 to 18 (from a high of 34 to a low of 15), says the NCES.

Of course, when it comes to homicides on school grounds, statistics are of little comfort. Those responsible for school security may need to know whether incidents are increasing, decreasing, or holding steady over time, but parents and educators are not concerned with trends; they want to know their kids are safe.

As students grow, so do security concerns. While active shooter incidents garner the most attention, school security officials spend most of their time working on less dramatic but far more common problems. In the 2013 – 2014 school year, for instance, NCES reported that 65% of public schools recorded one or more violent incidents. That is an estimated 757,000 crimes or approximately 15 crimes per 1,000 students enrolled. As alarming as that number is, it is important to note that between 1992 and 2014, violent and property-related incidents declined 82%, according to the U.S. Department of Justice National Crime Victimization Survey (NCVS).

For elementary schools, threats come largely from the outside world, which is why security at these schools generally concentrates on controlling access to the school building, both by physical means (single points of entry, secure locks, perimeter fencing, etc.) and by requiring faculty and staff to wear picture IDs.

As students age, the areas of concern proliferate and the focus turn increasingly inward to the students themselves. In 2013, for instance, the NCVS found that among students ages 12 to 18, 7% said they were threatened or injured with a weapon on school property, 12% said gangs were present at their school, and 22% reported that illegal drugs were offered, sold, or given to them on school property.

According to the NCES, high schools are doing what they can to reduce these numbers. Seventy-five percent of schools now use security cameras and many use metal detectors, although exact numbers are hard to come by. But, security measures and personnel cost money, and recent research by the Center on Budget and Policy Priorities indicates that most states have cut school funding in recent years—and some are planning further cuts.

In colleges and universities, significant offenses remain a concern, but things have improved. According to the U.S. Department of Education's Campus Safety and Security website, there were nearly 7,000 cases of aggravated assault on college and university campuses in 2005. By 2014, that number had dropped by a third to about 4,600 cases. Crime declined in several categories and overall criminal offenses dropped 40% from about 84,000 in 2005 to about 50,000 in 2014, despite a 20% increase in total enrollment.

One reason for this improvement may have been an increase in security forces. As a special report, "Campus Law Enforcement, 2011-12", by the U.S. Department of Justice notes, "Between the 2004-05 and 2011-12 school years, the increase in full-time campus law enforcement employees (16%) outpaced the increase in student enrollment (11%)."

Many colleges and universities also work closely with local police. In fact, notes the "Campus Law Enforcement" report, about 70% had formal written agreements with outside law enforcement. Such arrangements are especially valuable in urban settings. At the New Jersey Institute of Technology (NJIT), which does not have a fenced-off campus, the collaboration developed naturally. Because school security officers worked the city streets, says Charles Tighe, NJIT's deputy chief of police, "a lot of the neighbors in the area were calling our police department. We'd tell them, 'We're coming, we'll help you, but really in the future you should call the city police." Eventually it just made sense to institute a joint patrol, so now there is a designated car with one NJIT and one Newark city police officer patrolling the streets around the school. In the same spirit of cooperation, if an NJIT student calls 911 instead of the 4-digit school emergency number, Newark police alert campus security.

As important as it is to respond to calls, schools are also working to prevent problems. Most campus law enforcement agencies serving 5,000, or more students, had personnel designated to address general crime prevention, rape prevention, drug education, alcohol education, stalking, victim assistance, and intimate partner violence, and most offer free on-demand walking and vehicle safety escort services, according to the "Campus Law Enforcement" report.





ACTIVE SHOOTER INCIDENTS

COLUMBINE CHANGED EVERYTHING. Before Eric Harris and Dylan Klebold struck on April 20, 1999, schools did not pay much attention to unlocked doors, or to jokes and rumors threatening violence. Fire drills were the only exercises that helped students and teachers prepare for an emergency, there was no way to communicate quickly to everyone on the premises, and when police responded to an emergency, they followed standard operating procedure, setting up a perimeter to contain the problem before calling in whatever additional help was needed.

No more. Now schools routinely limit access to buildings, locking all but one door, which may even be protected by an armed security officer and a metal detector. Every mention of potential violence is taken seriously, including social media, and everyone on campus participates in exercises that help them practice what they have learned about responding to an active shooter. New communication systems are in place almost everywhere, and police tactics have been radically overhauled.

RIGOROUS THREAT ASSESSMENTS ARE CRUCIAL. Even before Columbine, school officials generally took time to consider how they might prevent or respond to likely threats. What Columbine, Sandy Hook, and Virginia Tech taught everyone is that it is not enough to plan for what's likely; schools have to prepare for "black swan events" – unpredictable incidents with enormous consequences.

Threat assessments focus on three distinct perimeters. The first perimeter is establishing that no one who belongs on campus, who has been hired by the school, poses a danger. In most primary and secondary schools, anyone who has unsupervised access to students must be vetted. What is called for, and what private security companies can provide, is a full background investigation that includes known associates, a psychological assessment, and drug screening.

Once the first perimeter is secure, the next step is to provide a secure exterior perimeter, which typically includes physical and/or electronic barriers to unauthorized entry, as well as a highly visible, trained, and preferably armed security force.

Whether the officers are provided by the school's police department, private security or both, their job is to patrol the grounds so that would-be attackers find no safe way in.

The third perimeter is the school itself. Ideally, both exterior and interior door frames should be metal-clad, open outward (so they can't be kicked in), and have locks with deadbolts that extend at least one and a half inches (a 3/4" throw can be opened with a flimsy credit card). Each building deserves at least one trained, armed security or law enforcement officer, making it clear that any threat of violence will be immediately and forcefully shut down.

In addition to these measures, cameras should be strategically placed around campus and monitored in real-time. Cameras that go unmonitored may help investigations after an incident, but the only way to prevent a suicide or criminal act is if someone trained to spot warning signs is watching a live feed.

Finally, if all else fails and there is an active attack, schools must be prepared to notify everyone immediately, and everyone must know how to respond. Virtually all schools instruct students, faculty, and staff on what to do in the event of an emergency and run practice drills periodically.

At the request of faculty, New Jersey City University (NJCU) recently provided special training so that faculty would know exactly what to do if there was an active shooter incident on campus while they were in front of a class. For anyone who missed the training, says University President Susan Henderson, one-page flyers with the same information were printed up and placed in all the classrooms.

To help schools notify people about an incident as quickly as possible, several firms now provide emergency communication systems. After signing in, designated school officials can instantly send out messages and instructions via email, phone calls, and texts. NCJU uses an opt-in system, which allows students to specify how they want to receive alerts.

Not everyone has to sign up for the system to be effective, explains Henderson. After the Virginia Tech shooting, research determined that if you reach even one in five students who has opted-in to the emergency system, the message gets out fast enough so that everyone quickly knows where they need to be.

Unfortunately, not all school districts or institutions can afford to fully implement all the best practices just outlined, but someone who understands emergency preparedness can ensure that limited budgets are put to good use.

The FBI's research disproved all the myths about shooters being loners, misfits, and oddballs, as did a study conducted by the Secret Service and the U.S. Department of Education. Shooters cannot be distinguished by ethnic background or social class. Few have had a history of violence, and most have come from stable, two-parent homes. Virtually all were responding to some kind of loss or failure, but 93% carefully planned their attacks, rather than acting in the heat of the moment.









PROTECT SCHOOLS

THERE WAS A TIME, NOT ALL THAT LONG AGO, when security officers could keep an eye on students by walking the halls of a high school and patrolling the grounds of a campus. They could not be everywhere, of course, but video cameras helped, allowing one officer to watch multiple sites.

Not anymore. Today, there is a vast area where students congregate out of sight of adults. According to the Pew Research Center, three-quarters of teens and 81% of teens older than 14 use social media, across a variety of social media sites. They use it a lot, and just how they use it keeps changing. In their 2015 Overview, Pew noted, "Facebook is the most popular and frequently used social media platform among teens; half of teens use Instagram, and nearly as many use Snapchat." Seven months later, a survey by the investment bank Piper Jaffray indicated that Facebook was no longer the leader among social media platforms for teens they interviewed; Instagram was, with Facebook a distant fourth.

LAW ENFORCEMENT HAS BEEN TRYING TO KEEP WATCH ON THIS FLUID, VIRTUAL WORLD. A 2015 Social Media Survey by the International Association of Chiefs of Police (IACP) found that 96.4% of the law enforcement agencies surveyed were using social media, and more than 85% reported that their efforts had helped them solve crimes. This police work was largely reactive, however; more about finding out what had happened than figuring out what was likely to happen.

That began to change when marketing companies that had been tracking social media for Madison Avenue turned their attention to the world of law enforcement. These geo-marketers had pioneered the use of "geo-fences," areas within which they could use publicly available data from a range of social media platforms to scan online conversations in real-time. Employing keywords as filters, they helped their business customers use location-specific information gleaned from social media posts to establish sales territories, localize advertising campaigns, and offer in-store promotions to nearby customers—among many other uses.

By 2014, companies such as Texas-based Snaptrends were working with municipal police, school districts, and security departments at colleges and universities, using geo-fences and keywords to identify possible security threats within a given school building, neighborhood, or stadium. There were some notable successes: high schools in Orange County, Florida, and Glendale, California, for instance, reported that pilot programs had allowed school officials to help students who had discussed suicide online.

A NEW APPROACH TO THE USE OF SOCIAL MEDIA. Such successes tend to obscure the fact that these services are only managing to scan a tiny fraction of the social media landscape, says Gary Margolis, a former chief of police at the University of Vermont and co-founder of Social Sentinel Inc. According to Margolis, only 1% to 5% of people have their location service turned on at any given time. "That means that if you're only looking in a geo-fence, you're missing 95% to 99% of the conversations," he explains.

Instead of using just geo-fences, Social Sentinel employs a sophisticated algorithm to connect social media posts to specific customers, regardless of where they are when they post. In addition, the company uses what Margolis terms, "a robust and comprehensive threat library" to filter the 850 million to one billion posts it scans each day. This library is made up of more than routine keywords and phrases. Margolis explains, "We've invested significant

resources to understanding the language of harm on social media, employing linguists, subject matter experts, staff with backgrounds in safety and security, and mental health experts who are knowledgeable about suicide and depression."

The company has also analyzed how people's communication styles differ depending on which social media platform they are using, and the algorithm is constantly being expanded and re-fined based on new data. "After the horrible tragedies in Dallas and Baton Rouge," says Margolis, "our antennas were tuned to understand the language of violence targeting law enforcement officers, and as a result of what we learned about how that was being discussed, we updated and evolved our library."

Many have raised privacy concerns about the use of social media monitoring. A recent headline in the Washington Post is typical: "Schools are helping police spy in kids' social media activity." Margolis explains that what a tool like Social Sentinel is doing is scanning the social media cloud for verbal patterns (including emoticons) that indicate a possible threat, not monitoring conversations.

Furthermore, the digital data being scanned by Social Sentinel, Snaptrends, and other companies is all made publicly available by the social media services themselves. Only Facebook denies public access to its individual user accounts, but Margolis notes, "People who want to talk about doing bad things to other people are generally posting things on megaphone platforms— you tweet or post something to the world—Facebook is used more to post things to family and friends."

It is also important to note that customers who use these services must take responsibility for how they use the information they are given. "It's up to our customers to take the information we give them and conduct their own investigation," says Margolis. In the California suicide prevention case mentioned above, for instance, the Snaptrends software alerted school security officials that a female student had included the terms "cutting" and "nobody will miss me" in social media posts. As the Washington Post reported, "Since the software gets a huge number of flags for words and phrases like these, the security staff delved deeper, investigating more posts by the student. They discovered that she had two conflicting social media accounts: one that told the story of a happy, normal girl, and the other of someone suffering from suicidal thoughts and depression. The school staff alerted police, who conducted a welfare check at the student's home and informed her father. She eventually went into treatment."

