School Safety Newsletter

Volume 2, Issue 1 August 2014

A closer look: How many Newtown-like school shootings since Sandy Hook?

June 19, 2014 http://www.cnn.com/2014/06/11/us/school-shootings-cnn-number/

(CNN) -- After the shooting on June 10, 2014 at an Oregon high school, many media outlets, including CNN, reported that there have been 74 school shootings in the past 18 months. That's the time period since the December 2012 massacre at Sandy Hook Elementary School in Newtown, Connecticut, where 20 children and six adults were shot to death.

The statistic came from a group called Everytown for Gun Safety, an umbrella group started by former New York Mayor Michael Bloomberg, a passionate and public advocate of gun control. Without a doubt, that number is startling. CNN took a closer look at the list, delving into the circumstances of each incident Everytown included.

Everytown says on its web site that it gleans its information from media reports and that its list includes school shootings involving a firearm discharged inside or on school grounds, including assaults, homicides, suicides and accidental shootings. CNN determined that 15 of the incidents Everytown included were situations similar to the violence in Newtown or Oregon -- a minor or adult actively shooting inside or near a school. That works out to about one such shooting every five weeks, a startling figure in its own right. Some of the other incidents on Everytown's list included personal arguments, accidents and alleged gang activities and drug deals. Here are the 15 Newtown-like incidents that have occurred between the Sandy Hook massacre and the June 10th, 2014 shooting in Oregon:

1. January 10, 2013 -- Taft Union High School in Taft, California: A 16-year-old student opened fire in class. He was targeting two classmates who he felt had bullied him, law enforcement said. One student was injured. The shooter was placed into custody after a teacher and campus supervisor persuaded the student to put down his firearm. Read: California sheriff: Youth who shot classmate felt he'd been bullied

2. January 15, 2013 -- Stevens Institute of Business and Arts in St. Louis, Missouri: A part-time student shot and injured a school employee then apparently shot himself, according to St. Louis police. Read: Police say student suspected of shooting college employee

3. January 31, 2013 -- Price Middle School in Atlanta, Georgia: A 14-year-old was shot in the head outside his school, police said. His mother told CNN affiliate WSB-TV that he was taken to the hospital. Atlanta Public Schools announced that another student had been taken into custody after the 1:50 p.m. shooting. Read: Student shot, wounded at Atlanta school

4. April 12, 2013 -- New River Community College in Christianburg, Virginia: An 18-year-old student drove to the school's campus inside a mall and began shooting at 1:55 p.m. on a Friday, police said. He wounded two women. Read: Student shot 2 before being subdued, police say

5. June 7, 2013 -- Santa Monica College in Santa Monica, California: A gunman killed four people during a rampage that began at a home near the college campus, police said. He opened fire in the residence where police discovered two bodies, then the gunman shot at a passing car and carjacked

Protecting our future through information sharing

In This Issue

another. The gunman forced the driver to drive onto the campus and shot two people in a passing vehicle, police said. Another victim was shot outside the campus library, authorities said. The gunman was killed by authorities. Read: 5 dead in California shooting

6. August 20, 2013 -- Ronald E. McNair Discovery Learning Academy, in Decatur, Georgia: A gunman fired shots and barricaded himself inside the elementary school. Antoinette Tuff, who worked in the front office, was hailed as a hero for engaging suspect Michael Brandon Hill. She managed to talk him into into giving up, and no one was injured, police said. Read: 'True hero' for handling Georgia gunman

7. August 30, 2013 -- Carver High School in Winston-Salem, North Carolina: A student injured another during a shooting that occurred at 2:45 p.m. during a planned fire drill, CNN affiliate WXII reported. Read: Police probe school shooting

8. October 21, 2013 -- Sparks Middle School in Sparks, Nevada: A 12-year-old opened fire with a handgun he took from his parents, police say. Jose Reyes injured two students and killed Mike Landsberry, a teacher and Afghanistan war veteran, authorities said. Reyes killed himself. Read: Students injured, teacher killed at middle school

9. December 13, 2013 -- Arapahoe High School in Centennial, Colorado: Karl Halverson Pierson opened fire on a Friday inside his suburban Denver high school, police said. The 18-year-old allegedly shot Claire Davis, a 17-year-old senior, who later died at a hospital. Law enforcement said that Pierson apparently wanted revenge against a faculty member because of a "confrontation or disagreement." Read: Teen opens fire at Colorado high school, police say

10. January 9, 2014 -- Liberty Technology Magnet High School in Jackson, Tennessee: A 16-year-old student shot a classmate in the leg as classes were being dismissed for the day, police said, according to CNN affiliate WBBJ. The student was treated for his gunshot wound, WBBJ said. Read: Victim shot as school was dismissed for day, authorities say

11. January 14, 2014 -- Berrendo Middle School in Roswell, New Mexico: A 12-year-old boy walked into the school gym, pulled a shotgun out of a bag and fired at students waiting for the school day to begin, authorities said. The boy wounded two. Read: Boy opens fire in gym, authorities say

12. January 21, 2014 -- Purdue University in West Lafayette, Indiana: Student Cody M. Cousins, 23, opened fire in the basement of the Electrical Engineering Building, according to the university. Cousins allegedly killed Andrew F. Boldt, the school said, and both were listed as seniors.

The school's police chief said that Cousins left the building right after the shooting, and a city police officer arrested him. Cousins was "booked on a preliminary charge of murder," Purdue Police Chief John Cox said. Read: Student surrenders after killing another student, police say

13. January 24, 2014 -- South Carolina State University in Orangeburg, South Carolina: A manhunt kicked off after a student Brandon Robinson, 20, was shot to death at the school, authorities said. "He was a very nice young man," South Carolina State University President Thomas Elzey said. "And it hurts. It hurts us all." Police arrested Justin Bernard Singleton, 19, and charged him with Robinson's killing, according to a statement from the South Carolina Law Enforcement Division. Read: Men argued before shooting, police said

14. May 23, 2014 -- University of California, Santa Barbara in Isla Vista, California: Elliot Rodger, 22, stabbed to death three people in his apartment, police said. Then Rodger fired into a deli and killed a young man inside the shop and shot to death two sorority sisters. Cheng Yuan Hong, 20; George Chen, 19; Weihan Wang, 20; Katherine Cooper, 22; Veronika Weiss, 19; and Christopher Michaels-Martinez, 20, lost their lives. Others were injured. Rodger committed suicide, leaving behind a long, hateful essay. Read: Timeline to 'retribution': Isla Vista killings planned for years

15. June 5, 2014 -- Seattle Pacific University in Seattle, Washington: A 26-year-old man who was not a student at the school was tackled by a student security guard after he killed one person and wounded two others, police said. Once the suspect was on the ground, other students jumped on top of him, according to authorities. Police told CNN affiliate KIRO that Aaron Ybarra was fascinated with school shootings and told investigators he had visited Colorado's Columbine High School where two students killed 12 students and a teacher in 1999. Read: Alleged school shooter interested in school shootings, police say

Monthly Webinars!

First Wednesday of Every Month at 10 am.

Next Webinar - Sept 10, 2014

(This month is an exception and will be the second Wednesday of the month.)

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email schoolsafety@isp.state.il.us

How to Survive a Cyberattack

Here's how a North Carolina district responded to a denial-of-service attack that came from one of its own schools.

theJournal.com, By Phil Hardin 07/16/14

At 7:45 a.m. on Monday, April 8, 2013, 23,000 network users in the Rowan-Salisbury School System's 35 schools were accessing their Web-based curriculum resources and administrative applications when suddenly all Internet connectivity stopped. The outage lasted for about an hour. Teachers had to quickly switch their lessons to a Plan B, since most had components that required Internet access.

Internet connectivity returned briefly, but suddenly went down again for another hour. The Internet would go down for a third time before school ended.

The Internet outages weren't due to hardware failures, Internet provider outages or network maintenance. The school district was under attack — specifically, we were experiencing a distributed denial-of-service attack, or DDoS. DDoS attacks, one of the most common forms of cyberattack, are designed to overwhelm a targeted IP address with numerous network requests in order to interrupt or suspend network service.

Each morning for the next four days, the district lost Internet connectivity around 7:45 a.m. The Internet would remain down for about an hour and would go down two more times each day. During the next three weeks, the school system was attacked multiple times a day on eight different days. Each attack caused a loss of Internet connectivity. A great frustration among students and staff ensued. Teaching and learning was being significantly impacted.

Identifying the Problem

The school system's Internet connection was a 1 Gb connection. It was provided by the state of North Carolina as part of the North Carolina Research and Education Network (NCREN). This network serves all the state's public education facilities, as well as many private colleges and universities and the North Carolina Office of Information Technology. The NCREN system is managed by the Microelectronics Center of North Carolina (MCNC), a nonprofit organization. During the three weeks of Internet outages, numerous conversations took place between the MCNC staff and the district's technology department. It wasn't until the third day of Internet outages that MCNC identified DDoS attacks as the cause of the outages. Data analysis showed that the district's network was being attacked with as much as 6.4 Gb per second. The attack was focused on the public IP of the district's firewall. The purpose of the attack was to disrupt Internet connectivity to and from the school district.

Unfortunately, MCNC wasn't able to stop the DDoS attack at the perimeter of the NCREN Internet connection. Stopping the DDoS attack at the perimeter is essential to mitigate its effect on a network. Instead, MCNC implemented several measures to try to mitigate the attacks. These helped preserve connectivity for the other organizations sharing the network connection line with Rowan-Salisbury, but Internet connectivity for the district continued to be disrupted.

The district got some help from a retired 3Com/HP network engineer, Larry Tolbert. He had over 30 years of network engineering experience and was very familiar with Rowan Salisbury's network. After the district leveraged several of its infrastructure components to obtain additional information about the DDoS attack and to block the attack at the perimeter of the district's network, Tolbert configured the district's TippingPoint Intrusion Protection System (IPS) to capture packet data of future attacks for analysis. He also configured the IPS to prevent future attacks from reaching the district's firewall and to send alerts to the technology department at the start of any future attack.

As we discovered, the DDoS attacks were coming from hundreds of malware-infected, remotely controlled computers located all over the world. This made it difficult to determine the responsible person, but the district needed to try.

Calling the Cops

The next step was to get help from local law enforcement. Sgt. Detective Roger Hosey, who worked with the FBI's Cyber Taskforce and had previously worked as a school district technology technician, knew the system and its network.

Champaign, Illinois announces its "proven track record" of keeping schools safe — with the statistics to prove it. The school superintendent is convinced and therefore, will recommend that the school board renew the School Resource Officer (SRO) program.

Reported 7/18/14 by the School Safety Law Blog by Professor of Law, Bernard James from Pepperdine University School of Law

http://schoolsafetylawblog.com/2014/07/safety-law-news-for-71814/

According to The Champaign News-Gazette on 6/9/14, Champaign Police Deputy Chief Troy Daniels reported the following decrease in police reports generated from Champaign Schools since the beginning of the SRO program:

Year	Police Reports Generated from Champaign Schools
2005—2006 (Year SRO program began)	348
2008—2009	148
2013—2014	52

http://www.news-gazette.com/news/local/2014-06-09/officials-hear-public-

Mia Langheim
School Intelligence Officer
School Safety Newsletter
Statewide Terrorism & Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail: schoolsafety@isp.state.il.us

How to Survive a Cyberattack (continued)

The attacks continued for a fourth week, and on that Wednesday, Sgt. Detective Hosey and another officer visited each of the district's six high schools to interview staff members. They suspected a student might be responsible for the DDoS attacks. The staff interviews didn't reveal any specific leads, but they did raise awareness within the schools that law enforcement was investigating the Internet issues.

Sgt. Detective Hosey suggested assigning each high school a specific public IP and changing the firewall's public IP again. The changes were designed to limit the impact on the system's Internet connectivity if an attack was focused on an individual high school's public IP. Also, giving each school its own IP might help make a connection between the person responsible for the attack and the high school being attacked.

After law enforcement visited the high schools, DDoS attacks stopped for the next 15 days. On May 16, though, an attack was made on one of the high schools. Sgt. Detective Hosey believed the person responsible for the attack was using an online resource to determine the new public IP assigned to the high school.

An Attack From Within

The district's Palo Alto Networks firewall contained extensive reporting data, which showed that two computers in a Career & Technical Education (CTE) computer lab at a high school had accessed the website, IP Chicken to find the public IP of the attacked high school. A four-hour review of the firewall's logs also showed that the same two computers accessed a website, xboot.net, that allows individuals to buy, schedule and launch DDoS attacks on any public IP address that the user designates. Sgt. Detective Hosey, the assistant superintendent of administration, and I met with the CTE computer lab teacher to try to determine which students had been using the two identified computers.

Unfortunately, the teacher had not used good classroom management and technology supervision practices on the day when the attack had been launched, and was only able to suggest a couple of students she believed "may" have been using the two computers. We asked the teacher to make sure she employed good classroom management and technology supervision practices in the future, and we asked her to keep the meeting confidential. Somehow, though, that meeting information was leaked at the school, and students in the class were made aware of the situation.

We configured the district's IPS system to send alerts if anyone accessed IP Chicken or xboot.net, and waited for the next attack. None came until November 2013, when an alert indicated that someone had visited xboot.net. Firewall and IPS logs showed that a personal iOS device had been used to access xboot.net via the wireless network at the same high school that was linked to the previous school year's DDoS attack.

Aerohive access points provided wireless connectivity in the schools. These devices provide detailed reporting, and the district was able to determine that the user accessing the DDoS attack website was in the high school's gym. Calls to the high school's administration and school resource officer resulted in the user being located in the gym. The browser history on the device, an iPod touch, confirmed that it had accessed the DDoS website — but no attack had been initiated. The student was one of the two that the CTE computer lab teacher had suspected. The school's administration and local law enforcement took charge of the situation.

Since the initial DDoS attack, MCNC has installed a chief security officer and is looking at solutions that will safeguard the network against events like this at the edge in order to keep such attacks outside the main network. The school district's IPS alerts remain in place, waiting for the next attack to occur.

http://thejournal.com/Articles/2014/07/16/How-to-Survive-a-Cyberattack.aspx?Page=1